DOCTORAL (PhD) DISSERTATION

E-commerce security and its regulation: Vulnerable individuals in e-commerce

by

Narmin Miriyeva

Co-supervisors:
Professor Dr. Mezei Péter, Ph.D.
Associate Professor Dr. Csatlós Erzsébet, Ph.D.

(Dissertation submitted to preliminary debate)

(Manuscript completed: 31 August 2023.)

Doctoral School of Law and Political Sciences

University of Szeged

Szeged, 2023.

Table of contents

Acknowledgements

This work is the result of the years that I spent here in Hungary at the University of Szeged, as a PhD student and later as a PhD Candidate.

Firstly, I am thankful for the opportunity to come here, to the centre of Europe - Hungary, and get a new degree with the help of the Hungaricum Stipendium scholarship program.

I am very appreciative to have had such amazing supervisors – Professor Dr. Mezei Péter and Associate Professor Dr. Csatlós Erzsébet throughout my research years, and for their patience and feedback on my first drafts. Because due to their scientific guidance and support, I was able to successfully complete this work.

Also, I am indebted to all my family members, whether abroad or in my home country, who supported me morally, mentally and financially during my research years of study.

And finally, I am grateful to myself for being so hardworking and purposeful and never giving up on pursuing my future aspirations.

Acronyms and Abbreviations

AI: Artificial Intelligence

Art.: Article

B2B: business-to-business

B2C: business-to-consumer

B2G: business-to-government

C2B: consumer-to-business

C2C: consumer-to-consumer

C2G: consumer-to-government

CJEU: the Court of Justice of the EU

CRD: Directive 2011/83/EU on consumer rights

CRM: customer relationship management

DGA: Data Governance Act Regulation (EU) 2022/868 on European Data Governance

DMA: Digital Markets Acts Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector

DPAs: Data Protection Authorities

DPD: Directive 95/46/EC on the protection of natural persons with regard to the processing of personal data and on the free movement of such data

DPIA: Data Protection Impact Assessment

DSA: Digital Services Acts Regulation (EU) 2022/2065 on a SM for Digital Service

DSM Strategy: Digital Single Market Strategy

ECD: E-commerce Directive 2000/31/EC on certain legal aspects of information society services

E-commerce: electronic commerce

E-communications: electronic communications

EDI: electronic data interchange

E-marketplaces: electronic marketplaces

ENISA: the European Union Agency for Network and Information Security Agency

e-PD: Directive 2002/58/EC on privacy and electronic communications

e-PR: E-Privacy Regulation

E-transactions: electronic transactions

EU: European Union

EUCA: Regulation (EU) 2019/881 on ENISA and information and communications technology cybersecurity certification (EU Cybersecurity Act)

G2G: government-to-government

GDPR: General Data Protection Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of data

ICT: information communication technology

ISs: information systems

L-commerce: local commerce

MCAD: Directive 2006/114/EC on misleading and comparative advertising

M-commerce: mobile commerce

MS: Member States

NISD: Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems

NIS2D: Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union

P2B Regulation: Platform-to-Business Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services

PID: Directive 98/6/EC on consumer protection in the price indication products

S-commerce: social commerce

SMEs: small and medium-sized enterprises

TEC: Treaty Establishing the European Community

T&Cs: terms and conditions

TFEU: Treaty on the Functioning of the European Union

the EU Charter: the Charter of Fundamental Rights of the European Union

the SM: The Single Market

UCPD: Unfair Commercial Practices Directive 2005/29/EC

UCTD: Directive 93/13/EEC on unfair terms in consumer contracts

WP29: The Article 29 Working Party

WWW: World Wide Web

WTO: World Trade Organization

Chapter 1. Introduction

Society is on the cusp of the digital world, which has been triggered by the explosion in information technology and, as a consequence, the rapid growth of the Internet. The phenomenal growth of the Internet and the World Wide Web has also influenced modification in the daily lives of users and the fate of entrepreneurs in online markets. The Internet have intensified the spread of the electronic revolution, and as a result of the collaboration, a new network revolution has entered the scene.

The conjunction of Internet networks, website designs, and computer devices created a new wave of trade: electronic commerce or e-commerce. This is expressed in any form of business transaction where the parties communicate electronically, rather than via physical exchanges. Electronic commercial transactions are one of the key components of e-commerce that are carried out outside of national borders by private individuals and commercial entities. The concept of e-commerce transactions consists mainly of three components: electronic means, commerce, and transactions. Electronic means are the way and route of sale and purchase. Commerce is the basic essence of the operations and their substance. The transaction is the goal and result of the operation or activities.[1]

Improvements in basic information technology and continuous entrepreneurial innovation in business and marketing assure that there will be as many changes in the next ten years as they have in the last two decades. The 21st century will be the century of digitally activated social and commercial life, the outlines of which can be barely seen at the moment. Assumably, e-commerce will ultimately affect almost all forms of commerce, and most of the trade by 2050, if not sooner, will be e-commerce.[2]

E-commerce is an appealing area for anyone who wants to generate new ideas or who would like to innovatively bring them to life. Major technological advances in computers and communications continue at a rapid pace. As a result, the deployment, full operation, and even concept of the applications made possible by advances in technology are inevitably

[1] Faye Fangfei Wang, *Internet Jurisdiction and choice of law: Legal practices in the EU, US and China*, Cambridge University Press, Cambridge, 2010, 1.
[2] Kenneth C. Laudon & Carol Guercio Traver, *E-commerce: business, technology, society*, Boston, Pearson, 2017, 8.

delayed and unfulfilled, at least for a while. E-commerce appeals equally to people with a passion for fundamental problems and a desire to make transformative contributions.[3]

Many researchers and executives see the rise of e-commerce as a distinct field of industry as the most important economic development of the period. The world is undergoing tremendous changes in a way business is done due to the rapid adoption of networking technologies by businesses. The new business environment created by e-commerce is not an imaginary vision of technocrats, but rather a new 'global order' in which millions of dollars are exchanged between parties every day. In formulating corporate strategy and developing value, the role of e-commerce is undeniable. In addition, it also transforms our society and culture as we know it.[4]

The retail world is on an unprecedented wave of innovation. Technology plays a significant role, of course, but it's not the only force at work. New business models are evolving that will have a profound impact on e-commerce and the wider retail value chain. At the same time, the attitudes and preferences of consumers are changing. Today's e-commerce consumer is largely directed by price and convenience: doing business with products that ship quickly. These basic preferences will still exist by 2026, but along with the shopping experience, consumer perceptions of the e-commerce experience will have changed dramatically.[5]

With the acceleration of digital transformation, the e-commerce landscape is becoming more dynamic. Along with taking on new roles of existing actors, new actors emerged. Some business, individual and country barriers to e-commerce have been overcome, but new ones have emerged. New opportunities have emerged to unleash the potential of e-commerce to increase consumer growth and wealth. E-commerce was primarily designed to enable repeat transactions between large companies and relied on configurable networks for electronic data interchange. E-commerce is now expanding to smaller businesses with the expansion of open networks such as the Internet and is increasingly used for transactions between firms and customers. Although the e-commerce landscape is still dominated in absolute terms by transactions between businesses, the current pace of uptake is on average faster in sectors

[3] Steven O. Kimbrough & D.J. Wu (eds), *Formal Modelling in Electronic Commerce*, Berlin, Springer, 2005, 1.
[4] Celia T. Romm & Fay Sudweeks (eds), *Doing Business Electronically: a global perspective of electronic commerce*, London, Springer-Verlag Limited, 2000, 1.
[5] Ovum Report, 'The Future of E-commerce: The Road to 2026,' 2017, 12.

such as accommodation or retail where consumers are a major player. These dynamics are supported by universal access to the Internet via mobile devices, as well as modern payment methods.[6]

E-commerce is based on Internet technology. Overall, internet technology and information technology are the protagonists of the game. Without the Internet, e-commerce would hardly exist. However, e-commerce is not only about business and technology. The third part of the equation for understanding e-commerce is society. E-commerce has important social implications that managers can only ignore at their own risk. E-commerce has questioned the concepts of privacy, intellectual property, and even national sovereignty and governance. Managers need to understand these social improvements and cannot afford to accept that the Internet is limitless, transcends social governance and regulation, or is a place where market efficiency is the only factor.[7]

However, concerns about the physical store's demise are overblown, as e-commerce is expected to account for only 21% of overall retail sales and 5% of food sales by 2023. To begin with, consumers prefer to purchase from the comfort of their own homes rather than going to the nearby shopping mall. Moreover, brick-and-mortar retailers are dealing with an increase in the complexity of stock-keeping units; in a world of ever-shorter product cycles and rapid innovation, stock-keeping units have expanded quickly. Furthermore, today's highly digital, well-informed customers have higher expectations for customer service and experience, necessitating both a greater time given to customers and better-trained frontline workers. Additionally, the rise of omnichannel experiences is altering the core purpose of physical stores. Stores are projected to provide a growing number of omnichannel services, such as in-store fulfilment and online purchase returns.[8]

The COVID-19 pandemic has further emphasised the move to e-commerce as people and businesses have gone online to deal with several lockdown actions and travel restrictions. The crisis has also highlighted the significant digital divide between and within countries that characterise the world and raised fears that digital transformation will lead to increasing digital divides and inequalities. In different trade deals, governments are giving growing

[6] OECD, 'Unpacking E-Commerce: Business Models, Trends and Policies', Paris, OECD Publishing, 2019, 32.
[7] Laudon & Traver, *E-commerce*, ix.
[8] McKinsey & Company, 'Future of retail operations: Winning in a digital era', Issue 2, McKinsey & Company, 2020, 4-9.

attention to the treatment of e-commerce. Given that countries are at very different stages of e-commerce readiness and offer different priorities for different trade policy objectives, their reactions to the changing environment vary considerably.[9]

Although consumer protection has constantly been concentrated on defending the weaker party - the consumer, modern data-driven services, regardless powerful and advantageous they may be, frequently seem to put the consumer in a worse position than before. Traders profit from behavioural findings provided by datasets that frequently compile information from users' full history of Internet interactions, including search histories, email and instant message histories, browsing patterns, or forecasts of financial state. Consumers must deal with ever-evolving option infrastructures that are constantly being updated to optimise engagement and conversion rates.[10]

Since consumers are typically the weaker side in the transactions, it is believed that they should have their health, safety, and economic interests protected. In their interactions with professional traders, all consumers are protected by consumer policy instruments. Nonetheless, certain consumer groups may be particularly vulnerable in certain circumstances and require additional safeguards. Consumer vulnerability may be influenced by societal factors or specific traits of certain customers or groups of consumers, including age, gender, health, digital literacy, numeracy, or financial condition. Although the current pandemic may have made certain forms of vulnerability worse, they already exist.[11]

People are increasingly giving personal information to service providers and online platforms, sometimes unintentionally, as internet services and social media become more widely available. In addition to assaults and fraudulent usage occurring often, the digitalisation of information and improved network connectivity provides additional difficulties for the protection of personal data.[12]

[9] UNCTAD, 'What Is at Stake for Developing Countries in Trade Negotiations on E-Commerce? The Case of the Joint Statement initiative' UNCTAD Research Paper, 2021, v.
[10] BEUC: The European Consumer Organisation, 'Towards European Digital fairness: BEUC framing response paper for the REFIT consultation', Brussels, 20/02/2023, 4.
[11] European Commission, 'Communication from The Commission to The European Parliament and The Council New Consumer Agenda Strengthening consumer resilience for sustainable recovery', Brussels, 13.11.2020 COM (2020), 696 final, 16.
[12] OECD, 'Measuring the Digital Transformation: A Roadmap for the Future', Paris, OECD Publishing, 2019, 575.

The misuse of their personal information to commit fraud is a concern for half of all European Internet users. About seven out of ten consumers worry that their information will be utilised for anything other than what it was intended for. 71% of Europeans believe that if they want to buy goods or services, their only option is to give their personal information. Almost all users from the EU believe that if their data is lost or stolen, they would like to be informed about it. Only 15% of respondents believe they have total control over the data they share online, while 31% believe they have no control over it at all. Individuals must maintain effective control over personal data in this rapidly changing environment. Every person in the EU has this fundamental right, and it needs to be protected.[13]

The choice of EU law as the study's foundation seems acceptable for two key reasons. First of all, even though the EU is a union of sovereign states, each of which has its national laws, all MS must abide by the EU's rules, which reflect the EU's consensus on appropriate legal standards. The doctrine of the direct effect of EU legislation supports this strategy. The CJEU has ruled through this doctrine that EU laws, including the GDPR, are directly applicable and should be construed consistently throughout the Union, with a few limited exceptions. Moreover, even though the legal, economic, and cultural fragmentation of the EU market is undeniable, there is a common perception and political trend that it is a single market. The concept of a single digital market has gained prominence in recent years on the political agenda of the EU. It is thought that more uniform legal regulations in the digital sphere will lower the administrative costs for EU enterprises and increase citizen protection.[14]

It would not be an exaggeration to state that current e-commerce transactions are an integral part of the lifestyle of online users, given the increasing use of technologies by the population. In this regard, e-commerce corporations can be sure that online consumers' requests will increase over time and will find some solutions through more advanced technologies such as distributed ledger technology and AI. Since online users are the main concern of the EU's DSM Strategy, their security and protection are also connected to e-commerce-related areas in general. The same online user may be identified as both a consumer and a data subject because e-commerce is a multidisciplinary field that can overlap

[13] European Commission, Directorate-General for Justice and Consumers, 'How does the data protection reform strengthen citizens' rights?' Publications Office, Factsheet, 2018, 1.
[14] Helena U. Vrabec, *Data Subject Rights under the GDPR With a Commentary through the Lens of the Data-driven Economy*, UK, Oxford University Press, 2021, 12.

with several legal disciplines. In fact, some online users may be more receptive and vulnerable given that not all users are equally qualified and able to participate in these online relationships. As a result, the concept of vulnerability will be investigated in this work in terms of the protection and safety of vulnerable online users in both the consumer and data protection law disciplines. Finally, the most recent legislative transformations, in the digital industries, notably those relating to e-commerce, will be conducted.

1.1. The aim of the research

The aim of this dissertation is to examine and define the concept of vulnerability and the position of vulnerable individuals in both legal disciplines of consumer protection and data protection. Comparing and analysing the disciplines of consumer and data protection law in relation to the protection and security of the concept of vulnerability for digital sectors could help to mitigate the risks associated with this concept in the future. Since online users take part in e-commerce transactions, the general field of e-commerce as well as its primary subcategories, particularly B2C and B2B, will be reviewed in light of recent EU consumer protection-related cases.

There will be attempts to define this concept and particularly the vulnerable consumer position in online interactions from the consumer protection law field because the concept of vulnerability is not fully recognized in academia. Several current CJEU decisions and prospective current consumer regulatory measures will be taken into consideration with the aim of depicting and defining the position of online vulnerable consumers.

Later, this concept in the field of data protection law will be reviewed with the aim of finding and determining the position of vulnerable online data subjects in the data processing. Regarding the digital transformation, the EU's capacity to implement and provide the regulatory frameworks for the Digital Single Market will be closely examined.

1.2. The research questions

The research question is regarded as an important initial move that serves as a compass for an investigation. It assists the researcher in linking his or her literature review to the types

of data that will be collected. As a result, many accounts of the research method include the formulation of a research question as a stage that aids in the prevention of haphazard data collection and review.[15]

One of the main reasons for addressing these research questions is the start of research on e-commerce as a separate area of law. As a result, the second chapter, which is more informative, begins with e-commerce as a multidisciplinary area of law, but it attempts to provide a starting place and niche for additional academic effort. Individuals are one of the key participants in e-commerce transactions, thus their safety and security are, have been, and will always be a priority for the EU. Since not all people are the same and as a result they can be differentiated by mental or physical weakness, age, gender, gullibility and other factors. These distinguishing criteria demonstrate that while not all individuals may be recognised as the average or standard, some group of individuals may be left outside the circle. Individuals with these distinctive characteristics may feel more susceptible and vulnerable when interacting with others online. Since there is no clear formulation of the concept of vulnerability as a whole, the necessity to find it and review the existing ones in academics arose.

Within the research process the following questions will be addressed for further solutions:

a) To what extent can EU define the concept of vulnerability and the position of the vulnerable individuals in the consumer protection law;

b) To what extent can EU explain the concept of vulnerability and the position of the vulnerable individuals in the data protection law;

c) To what extent can EU e-commerce deal with recent regulatory issues?

As can be seen from the research questions the solution will be proposed from the online individuals' perspective, as they are one of the active and susceptible participants in both consumer and data protection disciplines. However, the focus will not be on the typical average user group, but on a vulnerable group of individuals who are more likely to be more needy and unaware of ways to be identified and anticipated as 'the vulnerable' in order to obtain the necessary protection during online transactions.

[15] Alan Bryman, 'The Research Question in Social Research: What is its Role?' *International Journal of Social Research Methodology*, vol/10:1, 2007, 5-20.

1.3. The research objectives

Since there is no clear position on the concept of vulnerability and the vulnerable individuals both in consumer and data protection law disciplines, the following research objectives will be reviewed:

a) to define the position of the concept of vulnerability and vulnerable individuals in the consumer protection law;
b) to determine the position of the concept of vulnerability and vulnerable individuals in the data protection law;
c) to ascertain the latest legal regulatory reformations in the e-commerce related areas.

1.4. The sources of the research

European politicians started the process of constructing what is now known as the *European Union (EU)* to put an end to the recurrent and brutal battles that resulted in the Second World War. On May 5, 1949, ten Western European nations established the Council of Europe with the goals of advancing democracy, defending human rights, and upholding the rule of law.[16] The 1951 Paris Treaty, by which the six founding Member States (MS) founded the European Coal and Steel Community (ECSC), catalysed the creation of the EU. Later, in 1957, they ratified the Rome Treaties creating the European Economic Community (EEC) and the European Atomic Energy Community (EAEC or Euratom). That marked the start of the process that resulted in the creation of the EU. Since then, and before the Lisbon Treaty was signed in 2007, several further amending treaties have been signed, the most significant of which entered into force in 1987 with the Single European Act, in 1993 the Maastricht Treaty, 1999 the Amsterdam Treaty and in 2003 the Nice Treaty.[17]

The implementation of the Treaty of Lisbon on 1 December 2009 marked the conclusion of the most recent round of extensive EU treaty revision. The most difficult and protracted journey in the history of European integration was taken by the EU to implement

[16] History of the EU: Pioneers, <https://european-union.europa.eu/principles-countries-history/history-eu_en> accessed 15 Aug. 2023
[17] Jean-Claude Piris, *The Lisbon Treaty: A legal and political analysis*, UK, Cambridge University Press, 2010,7.

the reforms outlined in this most recent treaty. The process, which was initially started by the Laeken European Council in December 2001, included the following steps: the *Draft Treaty* establishing a Constitution for Europe was drafted in 2002-2003; the *Constitutional Treaty* was adopted in 2004; it was rejected in referendums in France and the Netherlands in 2005; the *Treaty of Lisbon* was negotiated in 2007; and finally, it was rejected in a referendum in Ireland in 2008. Among these changes was the EU's largest-ever enlargement from 15 to 25 MS in 2004, followed by an additional enlargement to 27 MS in 2007.[18]

The legal fact that the Union itself has organs with decision-making capacity, which was up until this point in dispute, expresses the Union as a legal entity. The Union 'shall have an institutional framework, [19]' which consists of seven major institutions, according to the Lisbon Treaty. The primary institutions now also include the European Council and the European Central Bank in addition to the conventional five institutions of the former European Communities - the European Parliament, the Council, the European Commission, the CJEU, and the Court of Auditors. The Union can act toward the MS and its citizens through these institutions and the enormous and intricate structure of subsidiary organs and other entities. The EU has access to a sizable variety of 'legal instruments for the enactment of legislative actions. Regulations, directives, and decisions - the three sets of documents that had a legal effect on the European Community - become the primary legal instruments of the Union following the Lisbon Treaty. A new hierarchy of the Union's legal acts was created by new provisions in the TFEU, which allow these documents to contain 'legislative acts', 'non-legislative acts of universal application', or 'implementing actions.' Advisory opinions, recommendations, strategies, declarations, resolutions, white papers, and numerous other types of reports are just a few of the other, more informal legal instruments that the EU's organs have created and continue to use.[20]

As stated in Art.1 of the TEU "By this Treaty, the High Contracting Parties establish among themselves a EU, hereinafter called the 'Union', on which the MS confer competencies to attain objectives they have in common. Also, the same Art. of TEU pointed

[18] David Phinnemore, *The Treaty of Lisbon Origins and Negotiation*, England, Palgrave Macmillan, 2013, 1.
[19] Consolidated Version of the Treaty on European Union OJ C 326, 26.10.2012, Art.13.
[20] Deirdre M Curtin & Ige F Dekker, 'The European Union from Maastricht to Lisbon: Institutional and Legal Unity out of the shadows', in Paul Craig & Grainne De Burca (eds) *The Evolution of EU law*, New York, Oxford University Press Inc., 2011, 165-166.

out that: 'The Union shall be founded on the present Treaty and the Treaty on the Functioning of the EU (hereinafter referred to as 'the Treaties'). Those two Treaties shall have the same legal value. The Union shall replace and succeed the European Community.' According to Art.6 (ex-Art.6 TEU): 'The Union recognises the rights, freedoms and principles set out in the EU Charter of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties. The provisions of the EU Charter shall not extend in any way the competencies of the Union as defined in the Treaties.'[21]

Art.2 of the TFEU defined the categories and areas of competence of the Union. Art.2 stated that: 'When the Treaties confer on the Union exclusive competence in a specific area, only the Union may legislate and adopt legally binding acts, the MS being able to do so themselves only if so, empowered by the Union or for the implementation of Union acts. When the Treaties confer on the Union a competence shared with the MS in a specific area, the Union and the MS may legislate and adopt legally binding acts in that area. The MS shall exercise their competence to the extent that the Union has not exercised its competence. The MS shall again exercise their competence to the extent that the Union has decided to cease exercising its competence. The MS shall coordinate their economic and employment policies within arrangements as determined by this Treaty, which the Union shall have the competence to provide. The Union shall have competence, by the provisions of the Treaty of the EU, to define and implement a common foreign and security policy, including the progressive framing of a common defence policy. In certain areas and under the conditions laid down in the Treaties, the Union shall have the competence to carry out actions to support, coordinate or supplement the actions of the MS, without thereby superseding their competence in these areas. Legally binding acts of the Union adopted based on the provisions of the Treaties relating to these areas shall not entail harmonisation of MS' laws or regulations. The scope of and arrangements for exercising the Union's competencies shall be determined by the provisions of the Treaties relating to each area.[22]

Art.3 of TFEU provided that: 'The Union shall have exclusive competence in the following areas: a) customs union; b) the establishment of the competition rules necessary for the functioning of the internal market; c) monetary policy for the MS whose currency is the

[21] TEU post-Lisbon, 16-19.
[22] Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, p. 47–390, Art.2.

euro; d) the conservation of marine biological resources under the common fisheries policy; e) common commercial policy. The Union shall also have exclusive competence for the conclusion of an international agreement when its conclusion is provided for in a legislative act of the Union or is necessary to enable the Union to exercise its internal competence, or in so far as its conclusion may affect common rules or alter their scope. In addition, Art.4 of the TFEU established that: 'The Union shall share competence with the MS where the Treaties confer on it a competence which does not relate to the areas referred to in Articles 3 and 6. Shared competence between the Union and the MS applies in the following principal areas: a) internal market; b) social policy, for the aspects defined in this Treaty; c) economic, social and territorial cohesion; d) agriculture and fisheries, excluding the conservation of marine biological resources; e) environment; f) consumer protection; g) transport; h) trans-European networks; i) energy; j) area of freedom, security and justice; k) common safety concerns in public health matters, for the aspects defined in this Treaty'.[23]

There are seven main sources of EU law, including a) the EU Treaties, particularly the TEU and the TFEU; b) secondary legislation created under the EU Treaties; c) 'soft law,' which consists primarily of non-legally enforceable instruments that may aid in the interpretation and/or application of EU law; d) related Treaties made between the MS; e) international treaties that the Union has negotiated using the authority granted to it by the EU Treaties; f) decisions of the CJEU and g) general legal principles and fundamental rights that form the foundation of the MS' constitutions. As a primary source of Union legislature, the TEU and TFEU together make up the 'constitution' of the EU. They have such effect in some ways even though they do not explicitly aim to establish the constitution of a federal state. Numerous protocols, annexes, and declarations follow both the TEU and TFEU.[24] According to Art.51 of TEU which states that 'The Protocols and Annexes to the Treaties shall form an essential part thereof,'[25] protocols and annexes have legal force within the framework of the Union. If a declaration is approved by the Council, it may be enforceable under Union law (as most are). An example of a non-legally binding agreement is the one reached at the Edinburgh Summit after Denmark's vote rejected the TEU. A decision and a declaration about Denmark were made at this summit, but not by the Council, but rather by the heads of state

[23] Ibid, Art.3.
[24] John Fairhurst, *Law of the European Union,* UK, Pearson Education Limited, 2016, 57-61.
[25] TFEU, supra note, 16-19.

and government gathered in the European Council. This is not a part of the Union's legal system and is more equivalent to an international agreement.[26]

Art.288 (ex-Art.249 TEC) of TFEU differentiated several legal acts of the Union. As it is said: 'To exercise the Union's competencies, the institutions shall adopt regulations, directives, decisions, recommendations and opinions.' The same article also makes the following distinction between the aforementioned legal acts: 'A regulation shall have general application. It shall be binding in its entirety and directly applicable in all MS. A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods. A decision shall be binding in its entirety. A decision which specifies those to whom it is addressed shall be binding only on them. Recommendations and opinions shall have no binding force.' Also, Art.289 of TFEU states that 'The ordinary legislative procedure shall consist in the joint adoption by the European Parliament and the Council of a regulation, directive or decision on a proposal from the Commission. This procedure is defined in Art.294. In the specific cases provided for by the Treaties, the adoption of a regulation, directive or decision by the European Parliament with the participation of the Council, or by the latter with the participation of the European Parliament, shall constitute a special legislative procedure. Legal acts adopted by legislative procedure shall constitute legislative acts. In the specific cases provided for by the Treaties, legislative acts may be adopted on the initiative of a group of the MS or of the European Parliament, on a recommendation from the European Central Bank or at the request of the CJEU or the European Investment Bank.'[27]

In terms of how much it can compel national governments to comply with its laws and demands, the EU is exceptional among international organisations. It has had a significant impact on each of its member nations as a comprehensive type of regional integration in which nation-states share sovereignty. The influence of the EU is felt in a variety of non-MS that fall under its sphere of influence, not just in those that are members.[28]

The main sources of the dissertation will be based on the sources of the EU law, both primary and secondary legislation. Since the sources of primary law, the treaties establishing

[26] Fairhurst, *Law of the European Union,* 57-62.
[27] TFEU, Art.289-294.
[28] Johanna Jonsdottir, *Europeanization and the European Economic Area: Iceland's participation in the EU's policy process*, Oxon, Routledge, 2013, 1.

the EU law, in particular, the TEU and the TFEU are considered as treaties defining the distribution of competencies between the EU and EU MS, their role in achieving effective learning outcomes is undeniable. Amendments to the EU treaties, protocols annexed to the founding and amending treaties, accession treaties of new countries to the EU, the EU Charter from the Treaty of Lisbon - December 2009 and the general principles of law established by the CJEU will also be taken into account when investigating topics related to the security and regulation of e-commerce. Concerning sources of secondary law, the regulations, directives, decisions, opinions and recommendations listed in Art.288 TFEU, as well as atypical acts such as communications and resolutions, white and green papers, which are not listed in Art.288 TFEU, will adequately be analysed and its results will be used for scientific purposes. Meanwhile, international agreements with non-EU countries or with international organisations are also an integral part of EU law, they will also be scrutinised during the research process. Since they can have a direct effect according to some judgments of the CJEU and their legal force is superior to secondary law, it is therefore important to comply with them.[29]

1.5. The methodology of the research

The research methods used in this dissertation would be legal analysis and comparative research methods. As John C. Reitz mentioned, 'the comparative method' is to focus on the similarities and differences between the compared legal systems, but in assessing the significance of the differences, the comparativist must take into account the possibility of functional equivalence. Comparative analysis is especially well-suited to draw conclusions about a) unique features of each legal system and/or b) commonality in how the law approaches the particular subject under study. By challenging the comparatist to explain the similarities and contrasts between legal systems or to consider their relevance for the cultures being studied, the comparative method has the ability to generate a more fascinating analysis.[30] That's why, in this dissertation two different law disciplines – consumer and data

[29] Sources of the European Union law, < https://eur-lex.europa.eu/EN/legal-content/summary/sources-of-european-union-law.html> accessed 03 Aug. 2023.
[30] J. C. Reitz, 'How to Do Comparative Law,' *The American Journal of Comparative Law*, vol.46/4, 1998, 620.

protection law - will be compared and distinguished with aim to define the concept of vulnerability and the position of the vulnerable individual's suitability in these disciplines.

This dissertation would be based on the type of qualitative research, especially on the documentary/document analysis method. Because due to the documentary analysis method it would be possible to review and analyse the work of lawyers, research reporters, legislation and case law.[31] Document analysis is a methodical process for studying or evaluating documents, both printed and electronic (computer-based and Internet-based). Document analysis, like other qualitative research methodologies, necessitates the examination and interpretation of data in order to extract meaning, gain insight, and develop empirical knowledge. Skimming (a shallow examination), reading (a detailed examination), and interpretation are all parts of document analysis. Thematic analysis and content analysis are combined in this iterative procedure. Information is categorised according to the main research topics through the process of content analysis. Emerging themes serve as the categories for investigation in a type of data pattern identification known as thematic analysis. The procedure entails rereading and reviewing the data with greater care.[32]

The functional method is optimistically supported by the supposed conclusion that the rules and concepts may differ, but that most legal systems will ultimately solve legal problems similarly. According to Ralf Michaels, 'the functional method' is a triple misnomer, to put it briefly. Firstly, there are numerous functional methods rather than just one ('the'). Moreover, not all purportedly functional approaches are actually 'functional' at all. Finally, some initiatives that assert their devotion to it don't even adhere to any discernible 'method'. In fact, the term 'functionalism' is used in a variety of contexts to achieve a variety of objectives, including understanding the law, comparing (tertium comparationis), emphasising similarities (praesumptio similitudinis), constructing systems (such as 'legal families'), identifying the 'better law,' unifying the law, and critically evaluating the legal systems. This range of 'functional methods' emphasises the significance of selecting an appropriate comparison approach based on the study purpose and research topic. Essentially, what and how the researcher compares are determined by the study question(s) and research interest. The goal behind functionalism is to examine how actual issues with resolving conflicts of interest are

[31] K. Zweigert & H. Kötz, *Introduction to Comparative Law*, Oxford, Clarendon Press, 1998, 2-34.
[32] Glenn A. Bowen, 'Document Analysis as a Qualitative Research Method' *Qualitative Research Journal*, vol.9, no.2, 2009, 27-32.

handled in various countries in accordance with various legal systems. In its most basic form, the functional method compares solutions to real-world issues involving competing interests rather than primarily rules.[33] It would be advisable to take advantage of the functional method, trying to find in existing legislative acts a basis for the current status of the concept of vulnerability, as well as the position and definition of vulnerable individuals in online transactions.

1.6. Contribution to scientific field

This dissertation's primary contribution consists of examining and distinguishing the concept of vulnerability and its legal implications from several legal perspectives, which have not yet been adequately studied on academic grounds. The success of this work lies in the ability to combine the concept of vulnerability from two very different legal disciplines - consumer and data protection law - which would help to understand this concept from various angles as a whole while keeping in mind its distinct qualities and characteristics. By viewing and comparing this concept from different legal disciplines, it would be more practical and understandable to draw a complete picture of vulnerability as a concept.

Most importantly, this study intends to add knowledge and practical value to the disciplines of consumer and data protection legislation, as well as to the field of e-commerce as a whole. Exploring this concept and providing a concrete perspective on it will benefit consumers and data subjects, as well as be practical and useful to traders and data controllers in general. Additionally, there is a chance that our effort will make traders and data controllers in the future more cautious and aware when interacting with this concept and vulnerable individuals in general. This dissertation also draws the attention of EU legislators to the need to better assess and review the current position of vulnerabilities and vulnerable individuals in both the area of consumer and data protection law.

1.7. Limitation of the research work

[33] M. Van Hoecke, 'Methodology of comparative legal research' *Law and Method*, 2015, 9.

Despite best efforts, like all other research documents, this study also has some limitations. First, because it is based on a type of qualitative research, especially the method of documentary analysis, the explanation of the considered concept of vulnerability is based on a theoretical rather than a practical real-life perspective. Furthermore, because the concept of vulnerability has not been fully explored in academia in a broad sense, there has been a lack of secondary sources of information and research materials. Finally, there were some language barriers in terms of interpreting and verifying the collected information and data, as all the EU MS have their own local languages.

1.8. The structure of the research work

In this dissertation, all work is summarized in 6 chapters. The dissertation began with an introduction, then the main chapters follow, and ends with a final chapter with research commentary in the conclusions.

In Chapter One, after the introduction, the focus is on the research questions, research objectives, research sources, methodology, contribution to the scientific field, research limitations, and research structure of the work.

In Chapter Two, the field of e-commerce will be addressed as a separate area of law with distinct features and structures. There will be some discussion of the benefits and drawbacks of e-commerce as a distinct field. In broad terms, numerous e-commerce categories will be explained depending on a variety of circumstances. Due to the availability of appropriate resources, the focus will be on the regulation of e-commerce from an EU perspective, in addition to the perspective of the numerous international organisations on the definition and importance of e-commerce.

Chapter Three will begin by examining the two primary types of e-commerce in terms of volume and quantity, namely business-to-consumer and business-to-business transactions. Following a quick introduction of the EU regulatory framework for consumer protection, the concept of average consumers will be redefined. Later, the notion of vulnerability and vulnerable consumers will be thoroughly addressed in terms of its definition and provisions in EU consumer protection law to determine if EU consumer law can adequately identify and protect vulnerable consumers in online transactions.

Chapter Four will provide a succinct summary of how technology advancements have influenced the development of privacy and data protection law. Later, while determining the status of data subjects in exercising their rights when processing personal data in accordance with GDPR regulations, the various rights of data subjects with pertinent court cases will be taken into consideration. In order to determine the extent to which EU data protection law can define and ensure adequate protection of vulnerable individuals during data processing, average and vulnerable individuals will be examined and analysed as the data subjects after the main provisions of the GDPR and the clarification of the fundamental rights of data subjects.

Chapter Five focuses on e-commerce security in general, with a particular emphasis on data processing security, network and communications security, and other significant regulatory developments in the EU. And the emphasis will be on determining to what extent existing security policies are adequate for providing a suitable environment for their users. The chapter's major section evaluates the present e-commerce strategy, particularly the DSM Strategy. Later, the approaches for regulating e-commerce-related fields will be explored, especially in light of the recent digital transformation.

The last part of the dissertation is the conclusion of the research findings with some recommendations for future accomplishments in keeping the interest of online users, whether online consumers or data subjects at the highest level.

Chapter 2. E-commerce as a multidisciplinary area of law

In this chapter, the field of e-commerce will be treated as a multidisciplinary area of law with its unique features and distinctive structures. Some insight into the advantages and disadvantages of e-commerce as a separate area will be given. In general, different categories of e-commerce will also be mentioned depending on various factors. The EU's regulatory approach to e-commerce will be in the spotlight due to the availability of relevant materials, although the definition and importance of e-commerce will take into account the views of many international organisations.

2.1. The meaning and the definition of e-commerce

Commerce is a primary economic activity implying trading or buying and selling of goods. There are two types of trading: physical trading and e-commerce. In a physical or traditional trading system, transactions are made through personal contacts, usually at a physical point of sale such as a store.[34]

There are many possible definitions of commerce. As *Burnham* argues, commerce can be best characterised as four fundamental activities by transferring the value of these activities, such as buying, selling, investing and lending. A sophisticated infrastructure has been developed to sustain these activities in the physical world that enables companies, consumers and governments efficiently to provide, pay and finance any business operation. Following the traditional definition of commerce, e-commerce encompasses the transfer of value through one of four principal activities over the Internet: buying, selling, investing, and lending.[35]

As a continuation of the electronic revolution, communication technology and business management have also undergone significant changes in the online world. These changes have had a great influence on the communication of people with each other and the way business transactions are conducted between organisations. Technological progress paired with internet-accessed customers is also driving massive growth of online business

[34] Henry Chan et al, *E-commerce: Fundamentals and Applications,* Chichester, John Wiley & Sons Ltd, 2001, 2-3.
[35] Bill Burnham, *How to Invest in E-Commerce Stocks,* USA, The McGraw-Hill Companies Inc., 1999, 2-3

transactions. During these interconnections, several buzzwords have emerged like e-commerce, which is more in demand in the digital world and even more in the interest of customers and commercial companies. E-commerce is integrated into our social and business life in a way that is difficult to distinguish. Since e-commerce is everywhere, it's impossible to ignore its role in embedded applications and the management process.

E-commerce is a system that embraces not only transactions that focus on buying and selling goods and services to generate income directly but also transactions that improve the generation of income, creating the request for these goods and services, attempting to support sales and customer service or ameliorating communication between business associates. E-commerce is found in the resources and structures of traditional commerce and extends the flexibility that e-networks offer.[36]

An important characteristic of any research project is a study of previous, applicable literature. A successful review provides a firm basis for information advancement.[37] Since there is no universally agreed-upon definition of e-commerce, it is important to review the literature on the definitions of e-commerce used by some of the major international organisations that are influential in global economic activity and some renowned academic associations that are significant in global research.[38]

2.1.1. The literature review of e-commerce in the researchers' work

While there is some agreement regarding its meaning, novelty, benefits and drawbacks, implications, and even its very nature, the word 'e-commerce' is not well described. The fact that there is no widely accepted standard concept of e-commerce is the reason for many differences in the expected growth of e-commerce. This is mainly because the positions of the Internet and its participants are very numerous, and their dynamic relationships change so quickly.[39] A review of research literature is a systematic, clear and reproducible method for the identification, assessment and synthesis of the current body of academics, scholars and

[36] David Kosiur, *Understanding Electronic Commerce,* Redmond, Microsoft Press, 1997, 3.
[37] Jane Webster, & Richard T. Waston 'Analyzing the past to prepare for the future: Writing a literature review', *MIS Quarterly*, vol.26, No.2, 2002, xiii.
[38] Zheng Qin et al., *E-commerce Strategy,* Hangzhou, Zhejiang University Press, 2014, 2.
[39] Subhajit Basu, *Global Perspectives on E-Commerce Taxation Law: Markets and the law,* Ashgate Publishing Limited, Hamphsire, 2007, 14.

practitioners' completed and documented work.[40] Literature research aims to examine the current state of knowledge in the area of interest, identify key authors, articles, theories, and results in this area, as well as determine knowledge gaps in this field of research. Today's literary research is usually conducted through computerised keyword searches of online databases.[41]

When researching the literature on e-commerce, the first step was to identify the relevant literature. Since the topic itself is modern and technology-related, research was first done on the Internet. The use of keywords such as 'electronic commerce', 'e-commerce', 'internet commerce' and 'web commerce' attempted to narrow the scope of the research. However, since e-commerce is inherently more multidimensional and multidisciplinary, this topic has its origins in different scientific disciplines. In addition, articles from major online database publishers were tracked and searched for the keyword, and the irrelevant ones were excluded.

The scholars *Ngai and Wat* excluded conference proceedings, master's theses, doctoral theses, textbooks, and unpublished working papers in their literature review of e-commerce and its classification. During a review of the e-commerce literature between 1993 and 1999, the researchers divided their findings into four main categories such as applications, technology issues, support and adoption, and other categories. It was found that no previous studies identified or evaluated the e-commerce study. The authors agreed that both researchers and professionals most often use journals to gather information and disseminate discoveries and represent the highest quality of science.[42] The latter direction and process of the researchers were implemented and applied while writing the literature review for the dissertation.

The term 'e-commerce' has been given so many different meanings by different actors, regardless of what the word 'commerce' contains, that the term cannot be used neutrally. In practice, one can think of different types of definitions for e-commerce, depending on the types of activities. It is further emphasized that e-commerce refers to the use of information

[40] Arlene Fink, *Conducting research literature reviews: From the Internet to Paper,* California, SAGE Publications Inc., 2014, 3.
[41] Anol Bhattacherjee, *Social Science Research: Principles, Methods, and Practices,* Textbooks Collection 3, 2012, 21.
[42] E.W.T. Ngai & F.K.T. Wat, 'A literature review and classification of electronic commerce research' *Information & Management*, vol.39, 2002, 415-429.

and communication technologies for the complete electronic value chain of business processes, and not to a technology or an application. Recognising the impact of e-commerce on the nature of economic transactions and, as a result, on the economy, requires understanding the relationship between technology and business process activity. When studying the definition of e-commerce, it can be assumed that at least one definition should be related to the problem of the transformation of economic activity, otherwise, in the commercial sphere, it is considered to be the application of new information technologies. In addition, the definition must be technology-specific, otherwise, e-commerce will not be different from e-transactions that have existed for many years, such as transactions by fax, or telephone.[43]

The phrase e-commerce is a confusing term that is frequently used to convey a variety of definitions, depending on the person's work role, professional orientation and context, focus product or service, and type of information technology employed. There are more than 30 different technologies that enable individuals or groups to conduct e-commerce. E-commerce is, by necessity, more than just the application of technology. E-commerce is portrayed as the seamless integration of information and technology across the full value chain of business processes that are carried out electronically and in a structured manner to achieve a business goal.[44]

E-commerce covers all aspects of business and market processes that have become possible due to the technologies of the Internet and the WWW. Like IS, e-commerce is multidisciplinary, borrowing computer science, psychology, economics, organisational theory, and natural sciences principles and theories, as well as from applied fields of research such as marketing, management, finance, accounting, engineering, and law. Many high-quality publications in domains including marketing, management, and computer science have been published and will continue to publish studies on e-commerce.[45]

Some scholars offer a very broad description of e-commerce, including all those communications of applications that support business activities. They emphasise e-commerce

[43] Alessandra Colecchia, 'Defining and measuring e-commerce: A status Report' OECD Working papers, Paris, vol.7, No.78, 1999, 9.
[44] Rolf T. Wigand, 'Electronic Commerce: Definition, Theory, and Context' *The Information Society,* vol.13/1, 1997, 5.
[45] Pratyush Bharati & Peter Tarasewich, 'Global Perceptions of Journals Publishing E-Commerce Research' *Communications of the ACM*, vol.45(5), 2002, 21-26.

as a strategy or business model rather than e-commerce as an application or technology. Private research businesses, particularly e-consultants, propose a more comprehensive definition of e-commerce, focusing on business processes and Internet commerce while distinguishing between business-to-business and business-to-consumer transactions.[46]

E-commerce is defined as the interchange of business information, the management of business relationships, and the conduct of commercial transactions over telecommunications networks, according to *Zwass,* one of the pioneers in this field. Distinguishing inter-organisational and intra-organisational business processes is sometimes both pragmatically and analytically futile in today's corporate world, as operational borders between organisations have blurred. As a result, e-commerce encompasses both sell-buy interactions and transactions between businesses, as well as corporate systems that allow trade within businesses. Through the integration of disciplines, solutions in one subject can be impacted by learning in another, allowing for scientific advancement.[47]

According to *Wigand,* e-commerce is a relatively up-to-date concept, and the literature and trade press does not appear to identify it as an electronic enterprise, electronic business, electronic marketplaces, and related notions. E-commerce, generally speaking, involves any sort of economic activity carried out through electronic connections. E-commerce varies from electronic markets to electronic hierarchies and also involves electronically assisted business networks and cooperative agreements (electronic networks). Typical fields of use are services within the tourism, banking, or insurance sectors, but also product delivery and customer services.[48]

Wang supported e-commerce, the idea of a recent wave of commerce created through the combination of internet platforms, website designs and computing devices. It can be found in any type of business transaction in which the parties communicate electronically rather than through physical exchanges. In addition, intangible objects and services, such as computer software, entertainment content, and information services, can be ordered, paid for, and distributed electronically. The traditional commercial social environment is changing due to e-commerce from an industrial economy where machines dominate production to an

[46] Colecchia,' Defining and measuring e-commerce', 9.
[47] Zwass Vladimir, 'Electronic Commerce: Structures and Issues' *International Journal of Electronic Commerce,* 1996, vol.1:1, 3.
[48] Wigand, *Electronic Commerce,* 1-16.

information-based economy where intellectual property is the primary source of value and there are no physical boundaries.[49]

Alongside its use as a business practice, academic research into e-commerce has grown. The evolution of computer networks has been described by other researchers as a fundamental technical and economic transition to the network age of computing. According to *Urbaczewski et al.*, a review of the literature on e-commerce revealed three main points of view: organisational, economic, and technological, each of which included a considerable number of obviously connected research studies.[50]

2.1.2. The literature review of e-commerce in the international organisations' reports

There are various approaches and viewpoints to e-commerce. The concepts used by some international organisations and nations, however, include elements such as the use of information and communication technology and the Internet as a means of communication, the initiation of transactions, the transition from one economy to another across borders, and e-payment.[51]

According to the *Sacher Report* of the OECD, e-commerce typically referred to all types of commercial transactions involving both organisations and individuals based on electronic data processing and transmission, including text, sound and visual images. It also applied to the impact that the sharing of commercial information through electronic means can have on the structures and processes promoting and regulating commercial activities.[52] While the Sacher Report did not specifically influence the EU's e-commerce law, it contributed to the global understanding of the challenges and opportunities associated with e-commerce.

Back then OECD in its Status Report mentioned that definitions of e-commerce provided by different sources vary considerably. Some included all electronically occurring financial and commercial transactions, including electronic data interchange (EDI), electronic funds transfers, and all credit/debit card transactions. Others restricted e-commerce to

[49] Wang, *Internet Jurisdiction and Choice of Law*, 3-4.
[50] Andrew Urbaczewski, Leonard M. Jessup & Bradley Wheeler, 'Electronic Commerce Research: A Taxonomy and Synthesis' *Journal of Organizational Computing and Electronic Commerce*, 2002, vol.12:4, 266-267.
[51] World Customs Organization, 'WCO Study Report on Cross-border E-commerce',2017, 7.
[52] OECD, 'Sacher Report', OECD Digital Economy Papers, No. 29, Paris, OECD Publishing, 1997, 20.

consumer retail transactions for which the purchase and payment take place over the Internet.[53] The principal intention of e-commerce, according to the OECD, was the development of a new form of the business environment in an electronic environment that is expected to have long-term effects. These included competition and productivity, costs, the resilience and mobility of companies, consumer behaviour, the regulation of commercial activities and the effect on the institutional frameworks regulating and promoting such activities.[54]

In the context of the WTO, e-commerce was first recognised at the Second Ministerial Conference in Geneva in May 1998, at which ministers asserted the main purpose of "a systematic work program to explore all trade-related problems associated with global e-commerce, especially those matters defined by Members."[55] In September 1998, the General Council set up the WTO Work Programme on E-Commerce.[56] The WTO described e-commerce in the sense of trade in services as a) the provision of Internet access services; b) the electronic provision of services; and c) the use of the Internet as a medium for the provision of delivery services in which goods and services are purchased over the Internet but ultimately distributed in a non-electronic form to customers.[57]

The United Nations Commission on International Trade Law has also attempted to define e-commerce (UNCITRAL). The UNCITRAL Model Law on E-Commerce promulgated in 1996 and updated in 1998, stated that an increasing number of international trade transactions are conducted through the exchange of electronic data and other forms of communication, collectively known as 'e-commerce,' which includes the use of alternatives to paper-based communication methods and the storage of electronic information.[58] While UNCITRAL's work has had a notable influence on the EU's e-commerce law, it is important to recognize that the EU has its own unique legal framework and decision-making processes.

---

[53] Colecchia, 'Defining and measuring e-commerce', 8-9.
[54] Puay Tang et al (eds), *The Impact of Electronic Commerce on the Competitiveness of SMEs in the EU,* European Parliament Directorate General for Research Directorate, 2000, 3.
[55] WTO, 'Declaration on Global Electronic Commerce', Geneva WTO Ministerial 1998: Electronic Commerce, T/Min (98)/Dec/2, 20 May 1998, 1.
[56] Yasmin Ismail, 'E-commerce in the World Trade Organization: History and latest developments in the negotiations under the Joint *Statement' International Institute for Sustainable Development and CUTS International*, Geneva, 2020, 1.
[57] OECD, 'Unpacking E-Commerce', 15-16.
[58] United Nations Commission on International Trade Law, 'UNCITRAL Model Law on Electronic Commerce, with Guide to Enactment 1996: with Additional Article 5 bis as Adopted in 1998', New York, United Nations, 1999, 1-17.

The EU's e-commerce regulations are developed through internal procedures within the EU institutions and MS, taking into account a wide range of factors and stakeholders. However, UNCITRAL's contributions have provided valuable guidance and contributed to the harmonisation of e-commerce laws globally, including within the EU.[59]

In 1999, the OECD formed an international working group to compile a statistically accurate and feasible description of e-commerce that could be used in policymaking. The working group came up with two concepts of e-commerce that included the following dimensions: a) the network used for e-commerce and b) the business processes associated with e-commerce. The broad definition includes all e-transactions, including the purchasing and selling of products or services over computer networks. Just one element of the narrow description varies, namely that the network used to order goods and services is the Internet.[60]

The OECD 2009 update included new terminology improvements to simplify and clarify e-commerce definitions. The word 'electronic transaction' has been replaced by the phrase 'electronic commerce transaction.' To avoid terminology difficulties, the term 'computer-mediated networks' has been substituted with 'computer networks.' Added the statement 'by methods specifically designed to receive or place orders' emphasizing that not all actions are cross-network oriented, only those intentionally aimed at commercial purposes. Manually placed orders via e-mail, phone, or fax were not included. The phrase 'may be conducted online or offline' was replaced by 'does not have to be conducted online.' As a result, the new and improved definition of an e-commerce transaction is the sale or purchase of goods or services over computer networks using specially devised procedures to accept or place orders. These methods are used to order products or services, but they are not required to be used for payment or the final distribution of goods or services. Enterprises, households, individuals, governments, and other public or private groups can all engage in e-commerce transactions.[61]

E-commerce has been a priority for policymakers since the mid-1990s. The OECD Ministerial Conference on E-Commerce in Ottawa in 1998 recognised e-commerce as a

[59] Arno R. Lodder 'Directive 2000/31 /EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market' in Arno R. Lodder and Andrew D. Murray (eds), *EU Regulation of E-Commerce: A Commentary*, Cheltenham, Edward Elgar Publishing Limited, 2017, 59.
[60] United Nations, 'United Nations Economic Commission for Europe: The Impact of Globalization on National Accounts'. New York, United Nations, 2011, 250.
[61] OECD, 'OECD Guide to Measuring the Information Society', Paris, OECD Publishing, 2011, 73.

global engine of growth and economic development. In 2016, the OECD Ministerial Declaration on the Digital Economy advocated for measures to 'stimulate and help decrease obstacles to e-commerce for the benefit of consumers and enterprises within and beyond borders,' according to the declaration.[62]

For its study, according to UNCTAD, the definition of e-commerce would include transactions and sales made through computer networks, utilising various formats and devices, including the sharing of web and electronic data, using personal computers, laptops, tablets and cell phones of varying complexity levels. Physical goods, as well as intangible digital products and services that can be delivered digitally, can be involved in e-commerce.[63]

According to WTO Special Studies, e-commerce may be simply defined as the production, advertising, sale and distribution of products via telecommunication networks. Most of the topic is confined to the Internet – the medium mainly associated with e-commerce. In e-transactions, the study distinguishes between three stages a) the searching stage, b) the ordering and payment stage, and c) the distribution stage. These interactions can take place between interested parties on an independent basis or involve transactions within companies.[64]

On December 13, 2017, at the Eleventh Ministerial Conference, 71 WTO members announced their intention to move forward on the WTO e-commerce front and issued the first Joint Statement on E-Commerce. The group declared that it projected to "initiate exploratory work together toward future WTO negotiations on trade-related aspects of e-commerce."[65] Following a year of consultations, the number of signatories increased to 76 WTO Members, who released a second Joint Statement in Davos on January 25, 2019 with the intention "to involve as many WTO members as possible and seek to achieve a high standard result that builds on existing WTO agreements and frameworks."[66] The EU, as a member of the WTO, participates in the negotiations and discussions on the rules of e-commerce. In addition, as

[62] OECD, 'Measuring the Digital Transformation', 352.
[63] UNCTAD, 'Information economy report 2015: Unlocking the potential of E-Commerce for developing countries', Geneva, UNCTAD Research Papers, 2015, 3.
[64] Bacchetta Marc et al., 'Electronic commerce and the role of the WTO', WTO Special Studies, No. 2, WTO, Geneva, 1998, 1.
[65] WTO, 'Ministerial Conference Eleventh Session Buenos Aires: Joint Statement on Electronic Commerce', WT/MIN (17)/60, 13 December 2017 (17-6874), 1/1.
[66] WTO, 'Joint Statement on Electronic Commerce', WT/L/1056 25 January 2019 (19-0423), 1/1.

the EU often aligns its policies with international norms and standards, the work of the WTO in the area of e-commerce can help shape the EU's regulatory framework in this area.

In its report on COVID-19, the WTO indicated that the global existence of COVID-19 and its impact on e-commerce can inspire increased international cooperation and the growth of online buying and supply policies. The epidemic has shown that e-commerce can be a valuable tool or solution for consumers. Small firms can benefit from e-commerce, which can act as an economic engine for both local and international trade by making economies more competitive. E-commerce for the trading of goods and services has been negatively impacted by the same issues that have generated supply and demand instability in the wider economy. As a result of these disruptions, orders have been delayed or cancelled entirely. During the pandemic, a slew of other e-commerce issues arose or worsened. Price gouging (increasing prices unnecessarily), product safety concerns, misleading practices, cybersecurity concerns, the need for more bandwidth, and development-related problems are among them.[67]

2.1.3. The definition of e-commerce

In a broad sense, e-commerce refers to the use of computer networks to enhance organisational performance. Some of the organisational efficiencies of e-commerce include increased profitability, increased market share, improved customer service, and faster movement of goods. E-commerce encompasses more than just placing an online catalogue order. It covers every facet of an organisation's electronic interactions with its stakeholders, or the people who have a say in how the organisation develops in the future. Therefore, setting up a website to support investor relations or corresponding electronically with college students who may become employees fall under the umbrella of e-commerce. In a nutshell, e-commerce refers to the use of information technology to improve interactions and transactions with all parties involved in an organisation. Customers, suppliers, government regulators, financial institutions, managers, employees, and the general public are some examples of these stakeholders.[68]

[67] Narmin Miriyeva, 'E-Commerce in the Time of Covid-19' in: Hajdu, Gábor (szerk.) *Rendkívüli helyzetek és jog: Kalandozások a jog peremvidékén a COVID-19 apropóján* Szeged, Magyarország: Iurisperitus Kiadó, 2021, 93-109.
[68] Richard T. Watson et al., *Electronic Commerce: The Strategic Perspective*, Zurich, The Global Text, 2008, 8.

The process of conducting business transactions that are currently carried out by various means electronically without prior agreement can be defined as e-commerce in the narrow sense. In this way, e-commerce supports traditional business models by allowing customers to evaluate and select their purchases in the same way as in a traditional. Their business decisions are only partially supported electronically.[69]

Although the basic definition of e-commerce appears to be simplistic, it has become increasingly sophisticated over the past two decades. Primarily, there has been a huge rise in the variety of e-commerce platforms. Nowadays, the spectrum of e-commerce platforms includes the e-commerce platforms of incumbent companies and third-party e-commerce platforms; the latter includes e-commerce platforms for 'goods' and 'services.' Furthermore, a centralised platform of e-commerce has developed from a marketplace into an ecosystem of e-commerce. As technology advanced, more business functions moved online, including advertising, marketing, logistics, finance, product recommenders, and social media influencers. Additionally, e-commerce systems that yield new business models have embraced innovations such as cloud computing, big data, the Internet of Things (IoT), Artificial Intelligence (AI), machine learning (ML), and blockchain. Big data analysis and AI are the most prominent of these technologies since such technologies can help analyse a large number of customers and predict future preferences. This can be used to provide suggestions for particular goods that are likely to be bought by customers, encouraging marketing and sales in turn. Finally, a large number of e-commerce operators have given rise to the rapid growth of e-commerce in many countries in the regions.[70]

E-commerce is not a new development for the European Commission, as businesses have exchanged business data over a range of communication networks for several years. But expansion and fundamental changes, driven by the rapid growth of the Internet, are merely accelerating. As reported by the European Commission, e-commerce is about doing business electronically. It is focused on the processing and transmission of data electronically, including text, sound and video. It covers a wide range of operations, including electronic trading of products and services, online digital content distribution, transfers of electronic

[69] Nabil R. Adam & Yelena Yesha (eds*), Electronic commerce; current research issues and applications*, Berlin, Springer Verlag, 1996, 13.
[70] UN ESCAP, 'Selected issues in cross-border e-commerce development in Asia and the Pacific', Studies in Trade, Investment and Innovation No. 91, United Nations publication, 2019, 4-5.

funds, electronic share trading, electronic waybills, commercial auctions, collaborative design and engineering, online sourcing, public procurement, direct marketing for customers and after-sales services. It includes both goods (consumer goods, specialised medical devices) and services (information services, legal services in the financial sector), as well as traditional activities (healthcare, education) and new activities (virtual shopping centres).[71] On June 8, 2000, the European Parliament and the Council of the EU adopted the E-Commerce Directive (ECD), which, despite its name, does not define e-commerce in general. On contrary, this Directive focused on the definition of the 'information society services,' 'service provider' and 'established service provider', and sought 'to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States.'(Art.1.1) [72]

The different definitions of e-commerce given above indicate that both in the narrow and broader sense, e-commerce can be specified. In short, the broader term includes doing business in e-commerce, while the narrower definition only applies to e-commerce transactions. Over time, different meanings provided by the same organisation have also changed. This indicates that the concept of e-commerce is complex and depends on the goal one wants to count. It is also important to point out that e-commerce is more than a technology. It is a business model based on the application of information and communication technologies to every part of the value chain of products and services.[73]

2.1.4. The distinction between e-commerce and e-business

Many authors do not strictly distinguish between e-commerce and e-business in their interpretations. However, the concept of e-business is more complex and changeable. Even in her analysis, editor *Matrigo* described e-business as a superset of e-commerce. E-business is the business practices that are part of a value network; approach the consumer cycle and

[71] Commission of The European Communities, Communication from The Commission to The Council, 'The European Parliament, The Economic and Social Committee and The Committee of the Region', A European Initiative in Electronic Commerce, Brussels, 16.04.1997, COM (97) 157 final, 2.
[72] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, 1–16.
[73] Basu, G*lobal Perspectives on E-Commerce Taxation Law,* 15.

use information and communication technologies (ICT) integrative way based on the network organisational and cultural laws of the economy.[74]

For a better understanding of e-commerce, *Bidgoli* distinguished between e-commerce and e-business. In his opinion, e-commerce means buying and selling electronically on the Internet, and e-business is an electronic transaction (for example, the exchange of information), which also includes e-commerce. E-business refers to all of a company's activities involving the sale and purchase of services and products through the use of computers and communications technology. Online shopping, sales force automation, supply chain management, e-payment systems, and order management are all examples of e-business activities.[75]

There is no universally recognised definition for e-commerce or e-business. Various terms are used to illustrate distinct perspectives and focuses of diverse people in different organisations and business areas. Commerce is characterised as embracing the idea of trade and large-scale international exchanges of goods. E-commerce can be understood to include the electronic medium for this exchange by association. Therefore, a general definition of e-commerce is the large-scale exchange of goods (tangible or intangible) between different nations over an electronic medium, such as the Internet. This implies that, on a macro-environmental level, e-commerce encompasses a full socio-economic, telecommunications, and commercial infrastructure. Contrarily, the definition of business is a commercial venture as a going concern. E-business, broadly speaking, refers to any aspects of an organisation's management and operations that are electronic or digital. These include both direct business activities that have an impact on the enhancement of efficiency and integration of business processes and activities, such as marketing, sales, and human resource management, as well as indirect activities like business process re-engineering and change management.[76]

The term 'e-business' is defined as the use of electronic means for the internal or external management of an organisation's business. Internal e-business activities include connecting the organisation's employees via the intranet to improve information exchange, facilitate knowledge sharing, and support management reporting. E-business activities also

[74] Julie Mariga (ed), *Managing E-Commerce and Mobile Computing Technologies,* USA, Idea Group Publishing, 2003, 20.
[75] Hossein Bidgoli, *Electronic Commerce: Principles and Practice*, USA, Academic Press, 2002, 5.
[76] Rana Tassabehji, *Applying E-Commerce in Business,* London, SAGE Publications, 2003, 6-7.

incorporate supporting customer service activities and collaborating with business partners, such as carrying out collective investigations, advertising a new product, and forming sales promotions. On the hand, e-commerce is about simplifying transactions and selling goods and services online, over the Internet or on another telecommunications network. This includes electronic trading in physical and digital goods, which often covers all trading phases, especially online marketing, online ordering, e-payments and online sales for digital goods.[77]

Stair & Reynolds asserted that e-business goes beyond e-commerce to cover all business-related tasks and functions, such as accounting, finance, marketing, production, and human resources operations, using ISs and the Internet to execute them. In their opinion, working with clients, vendors, strategic partners, and stakeholders also includes e-business.[78]

According to *Mohapatra*, although some interchangeably use e-commerce and e-business, they are distinct terms. A more detailed definition of e-commerce is a digital information processing technology for using e-communications in business transactions to establish, transform and redefine value-creating relationships between organisations and individuals. A more detailed definition of e-business is a transformation of enterprise systems to provide additional customer value through the application of technologies, ideologies and the computing paradigm of the digital economy.[79]

Some authors have described e-business as the practice of executing and organising essential business processes such as product design, procurement, manufacture, sale, order fulfilment and service delivery through extensive use of computer and communications technologies and computerised data. Meantime, e-commerce is observed to be a subset of e-business and includes 'the use of the Internet and other information and communications technologies for the promotion, acquisition and sale of goods and services.'[80]

According to *Awad*, e-commerce covers a wide range of purchases other than online buying. E-business, on the other hand, entails directly connecting important business structures to critical constituencies such as consumers, vendors, and suppliers via the Internet,

---

[77] Tawfik Jelassi, Albrecht Enders & Francisco J. Martínez-López, *Strategies for e-Business Creating value through electronic and mobile commerce Concepts and Cases*, Edinburgh, Pearson Education Limited, 2014, 4.
[78] Ralph M. Stair & George W. Reynolds, *Fundamentals of Information Systems*, Boston, Cengage Leaning, 2016, 20.
[79] Sanjay Mohapatra, *E-Commerce Strategy: Text and Cases*, New York, Springer, 2013, 8-9.
[80] Michael Chesher, Rukesh Kaura & Peter Linton, *Electronic Business & Commerce*, London, Springer-Verlag, 2003, 40-42.

Extranets, and Intranets. This entails utilising electronic data to boost efficiency and create value by forging new connections between businesses and their customers. E-commerce refers to transactions with anybody, at any time and from any location. It emphasises new business opportunities that contribute to increased transaction efficiency and effectiveness.[81]

2.1.5. E-commerce as a multidisciplinary and separate field

As a rapidly growing multidisciplinary field, e-commerce can be described as a meeting ground where researchers from various academic disciplines complement each other. Computer scientists can offer software agents that best match consumer preferences at the lowest cost. Marketing researchers can analyse the reaction of the customer to certain agents. On the other hand, economists may develop structures for the electronic market where certain agents communicate. Researchers in ISs, who are well qualified to understand the interactions between all the agencies involved in e-commerce activities, will provide useful insights into how the unique capabilities enabled by those agents can be harnessed. In addition, a multidisciplinary team may be organised by researchers from various academic disciplines, in which each member brings their own experience to better understand the e-commerce phenomenon. It is important to endorse various theoretical principles and research methods from different academic disciplines to fully capture multifaceted e-commerce phenomena.[82]

Sherif believed that e-commerce is a multidisciplinary activity that affects the behaviour of the participants and the relationships they build among themselves. In his adopted version, he defined e-commerce as a series of fully dematerialized relationships between economic operators. Accordingly, e-commerce can refer to physical or virtual goods (software, information, books, etc.) or user profiles in the same way that some operators base their business models on the systematic use of both demographic and behavioural data obtained through online transactions.[83]

---

[81] Elias M. Awad, *Electronic Commerce: From vision to fulfillment,* New Jersey, Pearson Education, Inc., 2004, 3-5.
[82] S. Lee et al., 'An Analysis of Diversity in Electronic Commerce Research' *International Journal of Electronic Commerce*, vol.12(1), 2007, 31-67.
[83] Mustafa Hashem Sherif, *Protocols for Secure Electronic Commerce*, AT&T Laboratories, Boca Raton, New Jersey Series, CRC Press LLC, 2004, 1.

The multidisciplinary nature of e-commerce research distinguishes it as a separate field of study. Both the creation of new e-commerce business models based on the latest advances in the global web and the development of technologies and business systems that facilitate the implementation of e-commerce are opportunities for e-commerce research. E-commerce research problems should be approached from two angles due to their complexity. The integration of information technology and business models is the first step in making them mutually beneficial. Furthermore, it is foreseen that the ongoing information technology revolution, particularly in the business world, will fundamentally alter the overall economic infrastructure of industrial organisations. There will be a huge demand for creative applications of new information technologies as a result of this industrial structural change.[84]

Rayport & Jaworski suggested various characteristics that describe e-commerce, such as the fact that it is about the flow of digitised data between parties. By connecting the flow of goods and services or the delivery of electronic orders, this exchange can portray how parties, particularly organisations and individuals, communicate with one another. The following feature of e-commerce is that it is technologically enabled. Transactional technology, particularly the use of Internet browsers, is used in e-commerce to complete transactions to offer technology-enabled client interfaces. The fact that e-commerce is electronically mediated is the next feature. Furthermore, e-commerce is shifting away from basic technological transactions and toward more technology-mediated connections. Unlike in the real marketplace, where human contact transactions are permitted, purchases in the 'market space' are controlled or mediated by technology, primarily for customer interactions. As a result, a company's performance is determined by how successfully screens and devices handle clients and their expectations. The final characteristic is that e-commerce encompasses all electronic-based intra- and inter-organisational operations that support market transactions directly or indirectly. E-commerce has an impact on the interaction between businesses and their external stakeholders - customers, suppliers, partners, competitors, and markets - as well as the internal approach to operational actions, procedures, and rules. E-commerce can thus be properly defined as a technology-driven trade between participants (individuals,

[84] M.J. Shaw et al., 'Research opportunities in electronic commerce' *Decision Support Systems*, vol.21, 1997, 149-156.

organisations, or both) as well as intra- or inter-organisational activities that contribute to such an exchange.[85]

On the other hand, e-commerce can be viewed as an application of utilising technology on the Internet. At the same time, it can be seen as a tool that enables organisations to raise productivity and cut costs. Three alternative definitions of e-commerce can be summarised in different ways. In terms of technology, e-commerce is the use of technology used to simplify and enhance business transactions using Internet-based websites. As a business phenomenon, e-commerce is used to include the opportunity to purchase and sell goods, services and information mainly on websites on the Internet. E-commerce is a value-creation tool for companies and customers and offers the opportunity to buy and sell products, services and information on primarily Internet-based websites.[86]

Understanding e-commerce as a whole is a daunting activity since there is no single academic discipline able to cover all of e-commerce. Speaking about e-commerce as involving three large interrelated themes has proven useful: technology, business and society. However, all of this happens because there are historical advances as in previous technological and economic revolutions. Initially, technology advances and then those inventions are commercially exploited. If the technology's commercial use becomes widespread, a host of social, cultural, and political problems emerge and society is forced to react.[87]

The analysis of e-commerce law must begin with a basic understanding of the law and its role in society as it has evolved. It necessitates an interpretation of terrestrial standards, social behaviour, and the rule of law implementation. Even if it means challenging such societal foundations as sovereignty and human rights, these principles must be applied to new circumstances, infrastructure, and contexts. The majority of legal concerns that occur as a result of the use of e-commerce can be satisfactorily resolved by applying common legal principles. For example, contract law, business law, and consumer law all extend to the Internet, email correspondence, e-banking, and cyberspace as a whole. Both improvements and additions to the law, which are the product of the new era are referred to as 'e-commerce

[85] Jeffrey F. Rayport & Bernard J. Jaworski, *E-commerce,* New York, McGraw-Hill, 2001, 2-3.
[86] Zinovy Radovilsky, *Business Models for E-Commerce,* Chennai, Cognella Academic Publishing, 2015, 3.
[87] Laudon & Traver, *E-commerce,* 38.

law.' E-commerce law is becoming a distinct field of study, with legal experts, monographs, and courses offered at every law school.[88]

As a result, e-commerce is a significant and rising part of the retail economy. Is there such a thing as an e-commerce field of law? It is believed there is a strong argument to be made that there is a body of law that can legitimately be called 'e-commerce law' and that can be researched as such. It is easy to come up with counter-arguments to the idea that there is such a thing as a consistent body of law. The conduct of e-commerce has led to the emergence of many legal problems that belong to different subject areas and have little in common. Alternative dispute resolution, consumer rights, contracts, copyright, jurisdiction over online disputes, patents, payments, privacy, property, regulated industries, taxes, telecommunications, and trademarks are among the topics covered. Authentication, domain names, electronic trespassing, and service provider liability are a few additional legal concerns that are similar to but do not fit comfortably within, any typical legal subject area. There is no reason why any of the different legal areas should not be brought together under the umbrella of e-commerce law. It is supposed that the common technological characteristics of the medium through which e-commerce is conducted are what bind these different aspects of e-commerce law together and make them worthwhile to examine as a coherent whole.[89]

E-commerce has a different meaning depending on the point of view from which it is viewed. E-commerce is the supply of information, products/services, or payments over telephone lines, computer networks, or other means from a communication standpoint. E-commerce, in terms of business processes, is the use of technology to automate corporate activities and workflows. E-commerce, from a service standpoint, is a technique for businesses, customers, and management to lower business expenses while improving product quality and speeding up service delivery.[90]

Three areas were discovered to help revitalise e-commerce during the development phase. Initially, there are new e-commerce platforms that are integrating with e-commerce, retail, advertising, and secure payment mechanisms. Furthermore, networks of all types of

[88] Alan Davidson, *The law of electronic commerce*, Cambridge, Cambridge University Press, 2009, 2.
[89] John A. Rothchild, *Research Handbook on Electronic Commerce law*, Cheltenham, Edward Elgar Publishing Limited, 2016, 2.
[90] Ravi Kalakota & Andrew B. Whinston, *Electronic Commerce: A Manager's Guide,* USA, Addison-Wesley Longman Inc, 1997, 3-4.

electronic, social, manufacturing, consumer, engineering, finance and legal networks have lessened the necessity for modular offices from nine to five as planned. Flexibility requires shorter reaction times and faster processes. Global operations that span many time zones are poorly suited to success with a 9-to-5 schedule. E-commerce enables manufacturers to focus on their core business and outsource other industries around the world to those who can produce the highest quality products at the lowest cost. Finally, companies are redefining their internal production and management functions to take into account the capabilities of new information technologies. This internal reengineering works well with e-commerce technology. The efficiency benefits achieved internally through reengineering can be scaled up to the company's competitive advantage in the marketplace.[91]

To allow a comparison between different countries, it is important to recognize the main drivers of e-commerce. Such key factors can be calculated using a variety of metrics that can reflect the development stages of e-commerce in the respective countries. The criteria by which one can judge the degree of development of e-commerce may be different, for example, technological factors that reflect the degree of development of the telecommunications system, providing enterprises and customers with access to the latest technologies. Moreover, there are political factors, including the government's role in creating policies, programs and resources to encourage the use and advancement of e-commerce and IT. There are also social factors used in the integration of IT education and training levels and development that enable both future customers and the workforce to understand and utilise the latest technology. The final factor is the economic indicators, which include the overall prosperity and economic health of the nation and the elements that contribute to it.[92]

E-commerce has expanded into large sectors of organisational and social interaction during the last decade, based on the technical foundation of the Web-Internet complex. This broad-based organisational and technical expansion requires classification to be properly understood and utilised. Commerce, collaboration, communication, connection, and computation are the five areas that describe the key characteristics of e-commerce. Commerce, the highest level of operation, encompasses the complete spectrum of customer-supplier relationships, from markets to long-term electronic hierarchies and supply webs.

[91] J. Christopher Westland & Theodore H. K. Clark, *Global Electronic Commerce: Theory and Case Studies*, Cambridge, MIT Press, 2000, 2.
[92] Tassabehji, *Applying E-Commerce in Business*, 8.

Collaboration is the next area that describes a fundamental feature of e-commerce. Then there's the communication area, which includes everything from one-to-one and one-to-many communication to narrowcasting small community contact, and lastly, mass broadcasting at absolutely no cost. The other most significant domain in describing e-commerce is connection. Popular software development frameworks, many of which are open-source, enable a wide range of businesses to take advantage of already produced software that is also compatible with their trade and collaborating partners. Computation is the final important part of the e-commerce domain. The most popular pay-as-you-go computing alternative is cloud computing. Many companies respond to their client's requests for dynamic business models and cost-effective fulfilment of their own customers' needs by providing sophisticated software products, software development frameworks, or infrastructure as a service.[93]

E-commerce impacts both the national and global economies overwhelmingly. Recent research studies indicate that e-commerce has a positive impact on the development of the overall economies of countries and will continue to grow this contribution to economies.[94]

2.1.6. E-commerce applications and systems

The word 'e-commerce applications' covers a broad range of applications. It encompasses everything from small online stores operated by shopping carts to large-scale B2B systems. Many of these applications, fortunately, start with a common set of technical requirements. These tasks include storing, upgrading, and extracting critical data from a data store (usually a database), rendering data in a standard format like HTML or XML, and communicating with users who will consume, manipulate, and process the data.[95]

E-commerce applications help and execute business processes in various business areas such as call centres and online stores. E-commerce applications have increasingly evolved to include sophisticated functional features through their graphical user interfaces to meet the increasing market requirements. Since the user interfaces are constantly modified to represent

[93] Zwass, Vladimir, 'Electronic Commerce and Organizational Innovation: Aspects and Opportunities' *International Journal of Electronic Commerce*, vol.7, no.3, 2003, 7-37.
[94] K. M. Rahman, 'A Narrative Literature Review and E-commerce Website research' *EAI Endorsed Transactions on Scalable Information Systems*, vol.5/17, 2018, 1.
[95] Jesse Legg, *Build powerful e-commerce applications using Django*, a leading Python web framework, Birmingham, Packt Publishing, 2010, 11.

the continuous evolution of the underlying business processes, users expect continuous guidance when using e-commerce applications. Furthermore, the user interfaces of e-commerce applications are built from the perspective of IT staff rather than business users.[96]

In e-commerce applications, there are two general techniques for personalisation. The buyer-driven method is the first technique, in which the client signs up for various services, fills out forms or questionnaires, assesses products, participates in surveys, and so on. The seller-driven strategy is the next technique, in which the e-shop owner is in charge of the adaptation. Pre-defined business principles, targeted internet advertising, and product cross-selling and up-selling are all used to serve content. The main stages of the personalisation process consist of data collection, data processing, and, the result of personalisation.[97]

Many popular e-commerce applications move through the development phases, including tradition, translation, and transformation. Customers visit a physical bookshop, choose some books from the shelf, and pay for them at the cash register, according to tradition. Customers visit an online bookshop, browse the web pages for books, and pay for them at the checkout page, which is a translation of the traditional business to an e-commerce model. Transformation is the shift to a newer, potentially more efficient model, such as the virtual bookshop, which can contain numerous additional services not available in the traditional model, such as a search engine, shopping cart, and data mining-based promotion.[98]

The widespread availability of online technology and the ease with which e-commerce applications can be accessed has forced companies to implement creative business models and to optimize their operational capacities and market competitiveness. E-shop, e-mall, e-procurement, e-marketplace, e-auction, virtual communities, value chain service providers, value chain integrators, partnership networks, knowledge intermediaries, and trust service providers are some of the emerging market-oriented e-commerce models. Apart from personalisation, the collaboration also has long been regarded as the most important component of e-commerce applications. It is often viewed as the catalyst and mechanism for

[96] Zou et al., 'Improving the usability of e-commerce applications using business processes' *IEEE Transactions on Software Engineering,* vol.33, no.12, 2007, 1.
[97] P. Markellou, M. Rigou & S. Sirmakessis 'Web Personalization for E-Marketing Intelligence' in Sandeep Krishnamurthy(ed), *Contemporary research in e-marketing,* USA, Idea Group Publishing, vol.1, 2005, 50-51.
[98] Chan et al., *E-commerce: fundamentals and applications,* 18-22.

social interactions, providing support for community cooperation, communication, and negotiation.[99]

E-commerce systems are fundamentally interdisciplinary and there are several implementation options. The structure of the e-commerce system consists of four parts. The initial part is e-commerce applications, typical examples of which are business transfers and e-marketplaces. Client computers are the second part, consisting of client devices, in particular their browsers, which are used to interactively connect to e-commerce applications. The third part is wired networks, which are used to transfer data in e-commerce. The last part is the host computer, which contains most e-commerce applications, except for client-side programs such as cookies and mark-up language user interfaces. User requests, such as checking or adding items to the cart, are processed by the host computer, which includes three types of software, namely web servers, database servers, and applications designed specifically for e-commerce transactions.[100]

The commonly used definition of a system is that a system is an actual or possible part of reality that, if any, can be observed. The e-business system and the e-information system are the two subsystems that make up an e-commerce system. Contracts, legal codes, and organisational frameworks are among the components of the e-business system. These issues are not addressed in either software or hardware. The e-information system, on the other hand, is made up of interconnected hardware and software elements. In this way, e-information systems contribute to a company's business operation and this system varies from other business ISs. Most business processes are automated by e-commerce ISs, particularly when products and services are intangible. Many ISs for conventional ways of doing business, on the other hand, just complement the company's business operation. Since e-commerce ISs are such an integral part of the way people do business, their implementation necessitates a close integration of the e-business and e-commerce systems.[101]

---

[99] Chien-Chih Yu, 'Service-Oriented Data and Process Models for Personalization and Collaboration' in e-Business, in K. Bauknecht et al. (Eds.), *E-Commerce and Web Technologies 2006*, LNCS 4082, Berlin Heidelberg, Springer-Verlag, 2006, 72-81.

[100] Wen-Chen Hu (ed), *Selected Readings on Electronic Commerce Technologies: Contemporary Applications, Hershey,* Information Science Reference, 2009, xx.

[101] J. Gordijn, H. Bruin & H. Akkermans, 'Integral Design of E-commerce Systems: Aligning the Business with Software Architecture through Scenarios' in H. de Bruin(ed) *ICT-Architecture in the BeNeLux*, 1999, 2.

Consumers go through several phases in the sales life cycle, and a good e-commerce system must solve all of them. The user's ability to search for and find products for sale, negotiate rates, terms of payment, and delivery dates, submit an order to the seller to buy the items, pay for the product or service, receive product delivery, and receive after-sales support is the essence of every e-commerce system. Product distribution may be in the form of tangible items delivered in a conventional manner (e.g., by a shipping company) or electronic goods and services (e.g., downloaded over the Internet).[102]

In comparison to the technologies used to construct e-commerce systems and applications, some technologies are more commonly associated with techniques or algorithms than with specific languages or software. Almost every type of information technology has been utilised in e-commerce, but the three most frequent are AI, information retrieval (IR), and business management. AI is the use of computer programs to simulate human intellectual functions such as thinking, learning, problem-solving, and decision-making. E-commerce has benefited from AI techniques such as data mining and data warehousing. The study of indexing, searching, and managing data is known as IR. For a long time, IR has been frequently used by computer systems such as digital libraries. Relevance feedback and other IR methodologies have recently been developed for use with e-commerce. Traditional trade has long employed business management techniques such as supply chain management and enterprise resource planning (ERP).[103]

2.1.7. E-commerce regulation

As e-commerce law is multidisciplinary, the regulation of this area cannot be achieved through a single legal framework - notably the ECD 2000/31/EC - but would rather encompass the unity of all different e-commerce-related legal areas. According to Art.1(5) of the ECD, which addresses the purpose and scope of the directive, e-commerce has an impact on several economic activities that fall outside this directive's purview, including taxation, games of chance (lotteries and betting transactions), and issues about agreements or behaviours covered by cartel law. In a similar vein, while falling under the purview of e-

[102] Ralph M. Stair & George W. Reynolds, *Principles of Information Systems*, USA, Cengage Learning, 2018, 307-308.
[103] Hu (ed), *Selected Readings on Electronic Commerce Technologies*, xxvi.

commerce, copyright and related rights, trademark rights, consumer protection, and the protection of personal data are all subject to a specific set of guidelines and laws. As the originator in this sector, the ECD standard rules related to various e-commerce issues, in particular online services, advertising, unsolicited commercial communications (spam), online contracts and online orders in the EU.[104]

The ECD lays out the fundamental guidelines for compulsory consumer disclosure, online contracting procedures, and rules for business communications. A fundamental tenet of the ECD is the internal market clause. It makes sure that online service providers are governed by the laws of the MS in which they are headquartered rather than the MS from which the service is accessible. The measures outlined in the ECD are rigorously confined to the bare minimum required to accomplish the goal of the proper operation of the internal market in accordance with the proportionality principle. The growth of e-commerce within the information society presents significant employment opportunities in the Community, particularly in SMEs, and would encourage economic growth and investment in innovation by European companies. Additionally, given that everyone has access to the Internet, e-commerce development would also increase the competitiveness of the European business. The ECD should ensure a high level of protection of the general interest objectives, particularly the protection of minors and human dignity, consumer protection, and public health protection, wherever action is necessary and in the area without internal frontiers as it relates to e-commerce.[105]

During the long-heated debates, it has become clear that the ECD could be a vital piece of legislation that will pave the way for the digital transformation of the European Single Market. It is notable in two ways: initially, because of its vast scope, and next, because of its overarching policy objectives. The ECD is remarkable for being the first omnibus legislative package from the EU to particularly address the phenomenon of e-commerce. While there is already a vast penumbra of the EU law in areas such as consumer protection, distance selling, digital signatures, taxation, competition law, privacy, telecommunications and intellectual property, all of which have had an impact on e-commerce, the ECD is a key instrument in

[104] Court of Justice of the European Union, 'Electronic Commerce and contractual obligations', Research and documentation directorate, 2020, 1.
[105] Directive 2000/31/EC, OJ L 178, Rec.2-8.

defining European e-commerce regulation policy and harmonising important legal areas that are major obstacles to the development of the Single Market.[106]

Beyond the ECD, the Consumer Rights Directive (CRD) 2011/83/EU also plays a significant role in harmonising and promoting national legislation on online contracts between consumers and merchants. The CRD established guidelines for the traders' obligations to provide consumers with clear, understandable information before entering into a contract. If a consumer is dissatisfied with the product, they have 14 calendar days under the CRD to withdraw from the contract.[107] The scope of Directive (EU) 2011/83/EU is expanded by amending Directive (EU) 2019/2161, which covers contracts where the seller provides or undertakes to provide digital services or digital content to the buyer, and the buyer provides or undertakes to provide personal information. Additional disclosure requirements are set out in Directive (EU) 2019/2161 for online market service providers concerning contracts that consumers enter into with various providers there.[108]

As part of the Single Market, the European Commission presented two directives in 2015 to make it easier to buy products, digital content and digital services from any EU member to address these issues. In May 2019, the European Parliament and the Council approved Directive (EU) 2019/771[109] on certain aspects of contracts for the sale of goods and Directive (EU) 2019/770[110] on certain aspects of contracts for the supply of digital content and digital services which both came into effect in January 2022. These directives harmonize important provisions of EU consumer contract law relating to products, smart products, digital content and digital services and ensure a high level of consumer protection.

---

[106] Lilian Edwards (ed) *The New Legal Framework for E-Commerce in Europe*, Oregon, Hart Publishing, 2005, vi.

[107] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance OJ L 304, 22.11.2011, 64–88.

[108] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules (Text with EEA relevance), PE/83/2019/REV/1, OJ L 328, 18.12.2019, 7–28.

[109] Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC (Text with EEA relevance.), PE/27/2019/REV/1, OJ L 136, 22.5.2019, 28-50.

[110] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (Text with EEA relevance.), PE/26/2019/REV/1, OJL 136, 22.5.2019, 1–27.

The General Data Protection Regulation (EU) 2016/679 (GDPR) [111], adopted on April 27, 2016, has given new impetus to EU data protection law to protect individuals whose data is processed in both the public and private sectors. The GDPR creates a system of fully independent supervisory authorities responsible for monitoring and enforcing compliance and gives individuals greater control over their data. In addition, the GDPR updates and harmonizes regulations, allowing businesses to reduce administrative burdens and benefit from increased consumer confidence.

The Digital Services Act (DSA)[112] and the Digital Markets Act (DMA)[113] are two legislative proposals made by the European Commission to modernise regulations governing digital services in the EU. The proposals were made by the Commission in December 2020, and a political agreement was reached on the Digital Markets Act on March 25, 2022, and the Digital Services Act on April 23, 2022. Together, they make up a single set of new regulations that will be used throughout the EU to create a safer and more accessible online environment. The DSA and DMA have two main objectives: (1) to establish a level playing field to promote innovation, growth, and competitiveness, both in the European Single Market and internationally; and (2) to create a safer digital environment in which the fundamental rights of all users of digital services are protected.[114]

2.1.8. Summary

Since e-commerce is characterised by a wide range of technology-enabled infrastructure possibilities and components, it cannot be limited to one discipline. To explore e-commerce's potential and prospects in the future, it is advisable to view it as a distinct field rather than a subset of e-business law. Whether it is online commerce or digital commerce, the bottom line

[111] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, 1–88.

[112] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance), PE/30/2022/REV/1, OJ L 277, 27.10.2022, 1–102.

[113] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance), PE/17/2022/REV/1, OJ L 265, 12.10.2022, 1–66.

[114] European Commission, The Digital Services Act package, <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> accessed 27 Aug. 2023.

is that the processes and structure are the same in their basic functionality as in e-commerce and therefore should be considered as terms that are often used interchangeably. Due to its unique characteristics as a multidisciplinary field of study, e-commerce law has incorporated this function into its systems and applications. For the continuous and consistent evolution of e-commerce, especially e-commerce systems and e-commerce applications, all components must be integrated and combined to achieve the desired results and prevent unforeseen problems. The latest regulatory moves in online marketplaces and digital services show that the e-commerce field is constantly trying to keep up with the latest digital transformations in the internal market. Thus, it makes sense to consider e-commerce as a separate area with multilateral levels of interaction, since it involves businesses, organisations and individuals.

2.2. The evolution of e-commerce transactions

E-commerce is considered online trading or using the internet for business. Other aspects of human growth and interaction are equally important, even as the Internet and its descendants are expected to become a critical component of any form of e-commerce.

The Internet can sometimes take a backseat to other elements in addition to a broadband connection, for example when there are other opportunities to connect people and organisations. Simply put, the ability of technology to reduce transaction costs is a specific deciding factor. The best and most thorough way to reduce the transaction costs associated with normal trading business processes is through e-commerce. This is the main reason why e-commerce is growing so fast and there is no going back. As more inventive and efficient IT applications grow as a result of e-commerce, it may lose some of its success, but it will be an expansion rather than a decline. Because of this, some authors define e-commerce broadly, using expressions such as e-business, e-enterprise, and internet marketing.[115]

Between evolution and revolution, there are important differences. Given that evolution is a slow transition, most managers are familiar with this topic. When we witness a revolution, we are entering uncharted ground where enterprises may fail and where unrecoverable sacrifices and novel approaches are needed. Simply put, a revolution is a historical alteration

[115] Cheng Hsu and Somendra Pant, *Innovative Planning for Electronic Commerce and Enterprises: A Reference Model*, Dordrecht, Kluwer Academic Publishers, 2000, 8.

of how people act and believe that results from the spread of catalysts for change, such as concepts or technological advancements.[116]

In line with the technological and innovation movement that plays an important role in the development of e-commerce, there are several phases in the evolution of e-commerce. The interpretations and opinions of numerous academic authors and scholars were taken into consideration in the research on the evolution of e-commerce. For this reason, merging the chronological evolutionary periods from different authors and the point of view of other scholars reconstructed a new chronological evolutionary time frame. As a result, the stages of the historical evolution of e-commerce can be divided into the following periods: a) the early years of e-commerce, from 1969 to 1995; b) the first wave of e-commerce, from 1995 to 2003; c) the second wave of e-commerce, from 2004 to 2007; and d) the third wave of e-commerce, from 2007 to the present.

2.2.1. The early e-commerce transactions

According to *Sims,* e-commerce originated in the 1960s, but it wasn't the kind of trade that we are familiar with today. Although business documents were routinely shared, orders and invoices were the two types of documents that were transferred the most. EDI produced a standardised structure for these commercial papers sent electronically, leading to the paperless exchange.[117]

Over the early e-commerce years, companies have used a form of EDI. When a business sends machine-readable data to another business in a predetermined format, this is known as EDI. In the 1960s, companies found that many of the documents exchanged were related to the delivery of goods, such as invoices, purchase orders, and packing slips. The high implementation costs were one of the difficulties faced by the EDI pioneers.[118]

EDI is a type of method of exchanging business documents in a common format from one device to another to capture important information and send it electronically. EDI, also

[116] T. Coltman et al, 'E-Business: Revolution, Evolution, or Hype?' California Management review, vol.44, No.1, 2001, 59.
[117] Lisa Sims, *Building Your Online Store with WordPress and Woo Commerce: Learn to Leverage the Critical Role E-commerce Plays in Today's Competitive Marketplace*, USA, Apress Media LLC, 2018, 3.
[118] Gary P. Schneider, *E-commerce,* Boston, Cengage Learning, 2017, 9-10.

known as ‘paperless exchange’ or ‘paperless negotiation’, was designed to significantly reduce the amount of paper used and reduce printing costs. As EDI has grown, more businesses were implementing it to enhance their procurement procedures and interactions with consumers and suppliers.[119]

The launch of the first satellite has accelerated the creation of the Defence Advanced Research Projects Agency (DARPA) by the US military to restore technological leadership. The ARPANET was first established in October 1969 through the exchange of information between two local universities. The National Science Foundation took over management of what was then known as NSFNet in 1990 and significantly expanded its boundaries by connecting it to CSNET (Computer Science) at North American universities and later to EUnet at all research institutes in Europe.[120]

The ARPANET’s goal was academic rather than military and allowed more academic institutions to link to it, creating the far-reaching structure that the military originally envisioned. The ARPANET was the first network to use a form of Transmission Control Protocol/Internet Protocol (TCP/IP) that is now used as the industry-standard protocol for connecting to the Internet. Without the creation of the ARPANET, the foundation of the network that is today known as the Internet would not have existed.[121]

The World Wide Web, which has produced a genuinely interactive world, is the focal point of change on the Internet. The WWW, proposed by Tim Berners-Lee at CERN in 1989, is an Internet service that uses hypermedia to organise information. A link to another document, full-screen video, audio, or photo can be embedded in any document. The majority of the Internet’s hypermedia content is carried through the WWW. A hypertext’s extension is hypermedia. In the interim, hypertext enables a user to follow a particular thread or subject by clicking on the highlighted text to pursue the chosen path.[122]

Soon after the WWW was established in 1993 a team of researchers created a windowed graphical user interface for the Internet. A window is a specific kind of computer programme that runs on users’ PCs and gives them an immediate Internet interface. The main feature of

[119] Qin et al., *E-commerce Strategy*, 7.
[120] Mahmud Akhter Shareef et al., *The proliferation of the Internet Economy: E-Commerce for Global Adoption, Resistance, and Cultural Evolution,* Hershey, Information Science Reference, 2009, 11.
[121] Sims, *Building Your Online Store with WordPress and WooCommerce*, 3.
[122] Bidgoli, *Electronic commerce*, 8.

the software was a web browser created by Mark Anderson and his research group called 'Mosaic', which was the world's first truly global website. In the same group of researchers, in 1994 created a browser 'search engine' to perform keyword searches called 'Netscape', which for a short time had a near-monopoly in the web browser market. However, Netscape's dominance of the market was later undermined by competition, particularly Microsoft's Internet Explorer.[123]

It is still debatable by whom and when the first e-commerce transaction took place. *Sims* claimed that Dan Kohn founded the 'NetMarket' website, which acted as an online marketplace for goods ranging from electronics to jewellery, in 1994. On August 11, 1994, according to the Smithsonian website, Dan sold Sting's CD for $12.48 plus shipping to a friend in Philadelphia who protected his credit card information using data encryption.[124]

The early success of e-commerce was a clear confirmation of the many information technologies that have evolved over the past 40 years, from the creation of the early Internet to PCs and local area networks. The near-ideal competitive market, where information about prices, costs, and quality is fairly distributed, an almost infinite number of suppliers compete with each other, and consumers can access important market information anywhere in the world, was first discovered by economists in the early years of e-commerce. Reducing the demand for ineffective advertising will help reduce retailers' cost of customer acquisition. The advertisements can also be modified according to the requirements of each client.[125]

2.2.2. The first wave of e-commerce transactions

The 'boom era' was the first wave of e-commerce to be mentioned in the marketplace. Generally, it began with rapid growth, followed by a rapid decline, commonly referred to as 'bankruptcy.' More than 12,000 internet companies were founded between 1997 and 2000, with a total investment fund of more than $100 billion.[126] This period after 1995 is known as e-commerce, which is based on the Internet. The germination stage is defined as the period from 1995 to 1997. At the time, the Web was mostly utilised for publishing and searching

[123] Colin Combe, *Introduction to E-business Management and strategy,* Oxford, Elsevier Ltd, 2006, 24.
[124] Sims, *Building Your Online Store with WordPress and WooCommerce*, 4.
[125] Laudon & Traver, *E-commerce*, 29.
[126] Schneider, *E-commerce*, 10.

product information, rather than for e-transactions. The majority of businesses did not receive venture money, and new e-commerce services were similarly rare.[127]

This stage of e-commerce was devoted to digital media transactions such as buying and selling. The focus at the time was on order flow and gross income. It was partly a chance encounter between customers and vendors who would never have met otherwise. Although the impact of this shift was minor, some of them should simply accept transactions that would have been made through paper orders and claim that the business was done online.[128]

The history of e-commerce would be impossible to imagine without Amazon and eBay, the pioneers of Internet-based e-commerce transactions. Amazon was one of the first e-commerce enterprises to sell things over the Internet, having been launched in 1994 by Jeff Bezos. Amazon was founded with the sole purpose of selling books, but as its business grew, it expanded its product offerings to include electronics, software, DVDs, video games, music CDs, MP3s, apparel, shoes, and health items, among other things. Cadabra.com was Amazon's first domain name. After becoming famous for its high-volume e-commerce approach, it was renamed 'Amazon.' The name was designed to imply an increase in transaction volume, similar to the world's greatest river.[129]

There is eBay, a completely new concept, whereby bidding consumers can buy and sell goods. eBay was launched in September 1995 and allows anyone to sell anything as long as it is not unlawful or in violation of its policies. In reality, eBay has struggled to keep up with its success and balance its online client growth with excellence in online customer service. The next level of eBay automation was performed in cooperation with customers. By offering frequently asked questions (FAQs) online, eBay offered what was considered 'self-service.' This FAQ has constantly been updated based on customer feedback and introduced a system that evaluates business transactions. Since eBay did not have direct communication for purchases, the trust of the users increased. This also lowered the odds of unsatisfied clients.[130]

Alibaba Group Holding Ltd., founded in 1999, is the world's largest e-commerce corporation in the Far East. Alibaba and its affiliates provide customers and companies with

[127] Qin et al., *E-commerce Strategy,* 7.
[128] Ravi Kalakota & Marcia Robinson, *e-Business 2.0: a roadmap for success,* USA, Addison-Wesley Professional, 2001, 3.
[129] Mohapatra, *E-Commerce Strategy,* 5.
[130] Ibid, 141.

e-commerce, shopping, local utilities, entertainment, healthcare, cloud computing and financial services.[131]

With the creation of the WWW, millions of people have been able to reach the resources stored on the Internet. Mainly due to the development of web browsers and search engines, Internet navigation has become easier. The commercialisation of the Internet has allowed entrepreneurs and computer enthusiasts the opportunity to develop business models that have drawn millions of customers.[132]

This allowed businesses to have a written and pictorial presence on the web. The term 'e-commerce' was coined in the early 1990s, when the internet became commercialised and consumers began flocking to the WWW to participate. E-commerce technology grew at a breakneck pace. A large number of so-called dot-coms, or Internet start-ups, also appeared. Nearly all businesses in developed countries had a web presence.[133]

The internet only became popular for commercial use in the late 1990s, when Microsoft released Windows 98, which included a full-featured internet browser and server. Businesses established websites presenting product information and providing trading platforms for goods and services in the 2000s, while individuals used email and instant messaging in addition to buying online.[134]

Electronic mail (or e-mail) was utilised in the first wave as a relatively unstructured communication method. For many dot-com enterprises that went bankrupt selling digital products was challenging during the first wave of e-commerce. The recording industry could not find a way to bring digital music to the Internet. As a consequence, an atmosphere of digital piracy, especially the infringement of the intellectual property rights of music artists, began to flourish. It also failed to deliver on the promise of e-books. Successful first movers have typically been large companies with an undeniable reputation and marketing, sales, and manufacturing expertise. On the other hand, the unsuccessful pioneers were less ambitious and less experienced in these areas.[135]

---

[131] Antonella Zarra et al., 'Sustainability in the Age of Platforms: Final Report' Brussels, Centre for European Policy Studies (CEPS), 2019, 23.
[132] Combe, *Introduction to E-business Management and strategy*, 10.
[133] Efraim Turban et al., *Electronic Commerce 2018: A Managerial and Social Networks Perspective*, Switzerland, Springer, 2018, 12.
[134] Faye Fangfei Wang, *Law of electronic commercial transactions: contemporary issues in the EU, US, and China*, London, Routledge Taylor & Francis Group, 2010, 4.
[135] Schneider, *E-commerce*, 11.

Yet e-commerce growth at this point was immature. Since all the businesses did not want to miss the chance to make money, they introduced and financed a significant number of ideas relevant to e-commerce. As a result, while a lot of poor ideas were heavily supported, many good ideas did not get the proper implementation. Deficiencies in the development of e-commerce appeared in 2000 and eventually suppressed e-commerce. The dot-com bubble burst.[136]

2.2.3. The second wave of e-commerce transactions

In the second wave, retailers expanded their international reach and began conducting business in new nations and languages. Language translation and currency conversion have been two major roadblocks in the global development of e-commerce. In the second wave, existing businesses began to use their internal capital to fund the incremental expansion of e-commerce potential. The increased usage of home Internet connections to download huge audio and video files is widely credited for motivating many individuals to pay extra money for a broadband connection during the second wave. Broadband speed increases not only make Internet use more efficient but also have the potential to change how people use the Internet.[137]

The internet, according to UNCTAD, can be characterised as an open, global network that connects computer networks to facilitate data flow between them by using several established protocols. The competitive environment for Internet services differs significantly from that of the telephone due to fundamental distinctions between the Internet and older, more established global telecommunications networks, some of which are over a century old. The first distinction has to do with the numerous functions that infrastructures and protocols on the Internet and telephony networks. The second difference between the Internet and older telecommunications networks is that, in contrast to telephone networks, where intelligent information on the Internet is located at the centre of the network, the Internet's core is relatively quiet and subject to a trend of commercialisation and declining prices, whereas the telephone networks are the opposite.[138]

---

[136] Qin et al., *E-commerce Strategy,* 9.
[137] Schneider, *E-commerce*, 11.
[138] UNCTAD, 'Information Economy Report 2005', New York, United Nations, 2005, 90.

Through rational thought and change, e-commerce saw its true spring in 2004. Good e-commerce ideas with clear and realisable business models remained after the dot-com bubble burst, and have made significant progress in recent years. The greater number of people who had access to the Internet, the higher size of online transactions became. Furthermore, for e-commerce operations, firms possessed immense influence and resources. As a result, B2B online sales have been continuously increasing, and e-commerce has entered a new era of rapid growth. The mature phase of e-commerce has been since Google went public.[139]

In 2005, social networks, as well as m-commerce and wireless applications, received a lot of attention. Social commerce channels have been added to e-commerce since 2009. On Facebook and Twitter, the best pattern of rising commercial activities can be seen. The growth of e-commerce, as well as its new business models and overall changes, is undeniable, as it is all linked to rapidly evolving inventive technology and the Internet.[140]

New technology arrived in the second wave, which provided prospects for new web firms. Web 2.0 is the umbrella term for these technologies, which encompasses software that allows website users to participate in the production, editing, and dissemination of content on a third-party website. Web 2.0 technologies are used by websites such as Wikipedia, YouTube, and Facebook. Salespeople began to use email as a major trend in marketing and customer loyalty techniques in the second wave, which was linked with B2C and B2B. The second wave realised the promise of accessible technology by supporting the legal transmission of music, film, and other multimedia items over the Internet. Apple Computer's iTunes is an example of a second-wave digital distribution corporation that caters to the needs of customers and their industries.[141]

2.2.4. The third wave of e-commerce transactions

E-commerce has been revolutionised again by the quick rise of Web 2.0, which began in 2007 with the release of the iPhone and other cell phones and continues to this day. The widespread use of mobile devices such as smartphones and tablets, the expansion of e-commerce to include local products and services, and the emergence of an on-demand service

[139] Qin et al., *E-commerce Strategy,* 9.
[140] Turban et al., *Electronic Commerce 2018,* 12.
[141] Schneider, *E-commerce,* 11.

economy powered by millions of apps on mobile devices and cloud computing have all had a positive impact on the e-commerce sector. This period can be viewed as a societal, technological, and business phenomenon all at the same time.[142]

The App Store began its revolution in July 2008, when it launched its latest products. This revolutionary technology has simplified communication between developers and Apple, making money by selling improved applications to end users. In the AppStore business model, Apple has always served as a software distribution channel. Developers could create whatever applications and software they think were essential to further fulfil the specific demands of consumers by opening Apple products such as the iPhone, iPad, and iTunes. Apple's App Store had implemented a novel e-commerce business model.[143]

A third wave in the growth of e-commerce began in 2010 as a result of several elements coming together. One of these factors was the growing number of high-speed mobile networks around the world that provide profitable connections between customers and businesses, as well as a critical mass of mobile users with smartphones and tablets, which for the first time allowed them to interact online with companies. With the advent of mobile phones and smartphones with Internet access, the third wave of e-commerce marked the beginning of m-commerce. Smartphones are cell phones that have a web browser, a big keyboard, and an operating system that let users run various software applications. These phones come with service plans that offer very high or even infinite data transfers for a set monthly price. M-commerce is now possible on a large scale for the first time since the growth of such devices and the affordable cost of Internet connectivity.[144]

Instead of being dependent on technological innovation and a focus on selling through traditional e-commerce solutions, the new growth in e-commerce is more about the need to create a robust business model that will promote value-added services to consumers and profitability to the company. The development of modern e-commerce is more often associated with traditional business than with the foresight of most dot-com companies and purely online strategies for doing business online. These companies range in size from large conglomerates to numerous small and medium-sized organisations that incorporate e-commerce into their overall business plan. Finally, as e-commerce has evolved, numerous ad

[142] Laudon and Trevor, *E-commerce*, 31-32.
[143] Qin et al., *E-commerce Strategy*, 9.
[144] Schneider, *E-commerce*, 11-13.

hoc standards have been developed or updated to track its activities and communications across various forms of e-commerce.[145]

2.2.5. Summary

It is noteworthy that e-commerce has always existed, albeit in different structures and forms using different technologies. However, the development of Internet technologies has greatly contributed to the growth of e-commerce. Ultimately, since the development of technology and the speed of evolution are interconnected, the more advanced the technology, the faster e-commerce will develop. For this reason, despite all the market downturns caused by the economic crisis, pandemics, rising inflation or other circumstances, e-commerce will continue to develop and contribute more and more to the commercial and technological community.

2.3. Advantages and disadvantages of e-commerce

Information and communication technologies always open up new opportunities for companies and customers. When it comes to entering global markets, e-commerce is rapidly becoming the vehicle of choice for corporations. Promoting the expansion of e-commerce will ensure economic progress and innovation. The right environment for e-commerce businesses to operate is critical to their growth and survival. Harmonizing processes for the cross-border movement of low-value e-commerce, including customs and other regulatory requirements, will help e-commerce flourish even more.[146]

An e-commerce transaction is defined as the sale or purchase of goods or services over a computer network using methods specifically designed to receive or place orders. Goods and services can be ordered using these methods, but the distribution of goods and services does not have to be done over the Internet. E-commerce sales include all transactions through web pages, extranets, or enterprise EDI networks. The comparability of estimates can be affected by methodological issues in measuring e-commerce, such as the use of different data

[145] Radovilsky, *Business Models for E-Commerce*, 6.
[146] World Customs Organization, 'WCO Study Report on Cross-border E-commerce', 5.

collection, and evaluation methodologies, and the extent to which transnational corporations participate in e-commerce.[147]

The e-commerce infrastructure has been constantly improved, and its economic and social importance has grown. E-commerce not only creates new retail and company ecosystems, but it also has an impact on and accelerates the e-commerce transition in traditional industries, as well as facilitating and pushing total economic transformation and upgrading. E-commerce is becoming a more active actor as it contributes to economic growth, job creation, the smooth transformation and renewal of established businesses, and the strategic development of new industries.[148]

E-commerce's potential to promote competition in retail markets considerably extends client preferences and supports product delivery innovation. On the other side, some e-commerce market characteristics might encourage or ease anticompetitive collusion and unilateral behaviour by economic actors. There is rising concern about the growth of dominating online platform operators who conduct business across numerous product groups and benefit from network effects and significant data-collecting benefits, among other things. Furthermore, in e-commerce industries, increased transparency and the use of automated tools will pose significant dangers to online businesses' competitiveness.[149]

The advancement of e-commerce is already affecting the company and consumer behaviour. The importance of ICT applications and services is growing across the whole e-commerce value chain. Information collecting, agreement, transaction, and delivery are the four steps of the e-commerce phase. At each stage, there are potential ramifications for consumers, businesses, and other groups, as well as governments.[150]

Two themes have influenced the EU's involvement in the rapid growth of Internet users. To begin with, the EU recognised that the Internet provides additional economic growth that cannot be influenced without interfering with the areas of the Internal Market where it is directly active. On the other hand, the EU recognised that the creation and spread of the

[147] OECD, 'A Roadmap Toward A Common Framework for Measuring The Digital Economy: Report for the G20 Digital Economy Task Force', Saudi Arabia, 2020, 28.
[148] United Nations Industrial Development Organization (UNIDO), 'BRICS Plus E-commerce Development Report in 2018', 2019, 12-13.
[149] Directorate for Financial and Enterprise Affairs Competition Committee: Cancels & replaces the same document of 4 May 2018, 'Implications of E-commerce for Competition Policy', Background Note, DAF/COMP (2018)3, 5.
[150] UNCTAD, 'Information economy report 2015', 4.

Internet had a direct influence on people's security, both as customers and as private persons. The EU has begun to regard e-commerce as a crucial weapon for maintaining the Single Market's competitiveness.[151]

E-commerce is driving a paradigm shift in business in a variety of ways. It decreases operational expenses at various phases of corporate activity, broadens the industry's reach, lowers entry barriers, and so increases competition. E-commerce also necessitates the acquisition of new skills by established businesses. The advent of e-commerce has several significant implications for consumers. First of all, consumers have more information about goods and prices for a wider range of things, allowing them to choose from a larger selection of goods at lower prices. In addition, consumers benefit from other welfare benefits of e-commerce, such as time savings.[152]

There are two types of e-commerce benefits found in the existing literature: tangible and intangible. Business efficiency, enhanced process automation, the transformation of the traditional market chain, a retained and expanded client base, lower operating expenses, and the acquisition of a niche market are some of the concrete tangible benefits. Improving client welfare and education, consumer loyalty, competitive advantage, and convenient shopping are examples of intangible advantages.[153] E-commerce has a plethora of benefits, which are only growing over time. The research scholars have identified both the advantages and disadvantages of e-commerce for organisations, individual customers, and society as a whole.[154]

2.3.1. Advantages to organisations

E-commerce offers new ways to manage supply and value chains, improve production, transportation, and delivery processes, and bring business partners together in a streamlined business operating environment. It allows organisations and people to purchase and sell goods, services, and information over the Internet. It assists businesses in lowering the cost

[151] Andrej Savin, *EU Internet Law*, Edward Elgar Publishing Limited, Cheltenham, 2013, 2.
[152] OECD, 'Electronic and Mobile Commerce', OECD Digital Economy Papers, No. 228, Paris, OECD Publishing, 2013, 7-13.
[153] Joze Kuzic, Julie Fisher & Angela Scollary, 'Electronic Commerce Benefits, Challenges and Success Factors in The Australian Banking and Finance Industry' *Poland, ECIS 2002 Proceedings,* 2002, vol.60, 1608-1609.
[154] Tassabehji, *Applying E-Commerce in Business,* 8.

of customer service while improving service quality and enhancing the organisation's ability to manage client relationships efficiently.

Businesses, particularly SMEs and micro-companies would have additional opportunities. They will have access to new markets beyond national and even European borders. Businesses can improve their productivity by making more extensive use of internet resources and having access to cloud storage. A high-performance European Digital market would help the EU compete more effectively with the rest of the world by giving it a competitive advantage built on expertise, a highly skilled workforce, and progressive economic and social models.[155]

Managers must make appropriate use of the enhanced information accessible to them regarding the company's external and internal operating environments to succeed in e-commerce. E-commerce is based on the effective use of knowledge management, which is made possible by the use of information technology. E-commerce can be explained as a way for a corporation to make better use of the improved knowledge that is available to management. Through the smart use of information technology and human resources in the company, management may improve the efficiency and effectiveness of production, sales, and marketing activities.[156]

One of the most significant advantages of e-commerce is the introduction of new options to start a business creatively. The new business models allow entrepreneurs with little capital and experience to start and grow enterprises quickly. Many entrepreneurs make a lot of money online, especially when they use unique business strategies. E-commerce has the potential to foster innovation, leverage new business models, enable small enterprises to compete with large ones and implement distinctive business strategies. With direct consumer engagement and better customer relationship management, e-commerce has improved customer service and relationships. By providing e-procurement, e-commerce also gives lower rates, upgraded quality, improved brand image, and effective procurement with a competitive edge, saving time and money.[157]

---

[155] European Commission, 'A coherent framework for building trust in the Digital Single Market for e-commerce and online services', Commission Communication to The European Parliament, The Council, The Economic and Social Committee and The Committee of The Regions, Brussels, 11.1.2012, COM (2011) 942 final, 3.
[156] Kenneth Smith & John Paul Kawalek. 'Business ethics and E-Commerce in contemporary society' in *Re-Imaging Business Ethics: Meaningful Solutions for a Global Economy*, 2015, 17-16.
[157] Turban et al., *Electronic Commerce 2018,* 15.

E-commerce offers huge savings due to the lower cost of brick-and-mortar companies. Electronic trading eliminates the majority of the paperwork needed in the job because order placement, delivery, payment, and service requests all take place in an electronic format directly on the e-commerce server. It is feasible to considerably cut the price of maintaining a business location as well as all other necessary overheads. Shipping costs are decreased in two ways. To begin with, the cost of paper-based information or document exchange is replaced with substantially reduced electronic distribution costs in an e-commerce transaction since the data is transmitted electronically. Moreover, as each part of the industrial value chain is bypassed, a physical distribution connection and associated inventory-carrying expenses are removed.[158]

Businesses will gain from social commerce in a variety of ways, including increased revenue and profits, wider candidate coverage, faster and more cost-effective hiring, improved internal relationships (e.g., by boosting productivity and employee satisfaction), and free advice for small businesses from larger businesses and experts (e.g. through LinkedIn groups). Additionally, s-commerce lowers costs through innovative methods like employee and business partner collective knowledge, enhances cooperation, and fortifies relationships with both internal and external stakeholders (e.g., by using blogs, microblogs, and wikis). S-commerce benefits include quick and inexpensive market research, customer, employee, and business partner input gathering, the development of small consumer groups at minimal cost, and entry into extremely small markets with brand goods. Unquestionably, s-commerce plays a significant part in growing market share and profitability, building brands through social media discussions and promotions, and managing a company's and brand's online reputation.[159]

It has been argued that using e-commerce offers a variety of opportunities for firms and organisations to benefit, starting with a decrease in transaction costs. An organisation's operating structures, trade connections, knowledge, and strategic skills in the marketplace may be impacted by various interconnected e-commerce benefits that follow from the lowering of transaction costs. The value that businesses in developing nations might expect

[158] Bharat Bhasker, *Electronic Commerce: Framework, Technologies and Applications,* India, McGraw Hill Education, 2013, 6-10.
[159] Efraim Turban et al., *Social commerce: Marketing, Technology and Management,* Switzerland, Springer, 2016, 14.

or receive from e-commerce can be broadly categorised into three goals: a) strategic, b) informational, and c) operational. Strategic advantages are tied to increasing the organisation's business performance. Improved market information and communications have informational benefits. The attainment of cost savings and operational efficiency are related to the development of operational advantages, which support the market distribution of a company's goods or services. The corporation can acquire operational benefits, align its strategies, and optimise its processes to gain knowledge and competitive advantage because all three of these advantages appear to be interrelated.[160]

An e-commerce website can assist a company draw in new customers in untapped markets. This is one of the main justifications offered by organisations for creating a website. By eliminating or reducing time-consuming and labour-intensive processes in the order and delivery process, more transactions can be completed in the same amount of time and with improved accuracy. Businesses may reduce the requirement for inventory at all intermediate manufacturing, storage, and transportation stages, from raw materials to safety stocks and final products, with enhanced speed and accuracy of client order details. Since electronic connectivity and communications are already created, the flow of information is accelerated when businesses and their clients are connected through e-commerce. As a result, communication between the buyer and seller can happen fast, directly, and efficiently.[161]

2.3.2. Advantages to individuals

Over the past years, e-commerce has offered clients a wealth of advantages and prospects. Customers that engage in e-commerce have the opportunity to get better value in a more convenient method as well as experience even wider choices, including direct access to international markets. Consumers now possess the tools necessary to communicate with a product or service supplier and the demand side of the market. More generally, there are significant prospects to create a genuinely global e-commerce sector powered by consumers

[160] Richard Boateng & Robert Hinson, 'E-commerce and socio-economic development; Conceptualizing the link' *Article in Internet Research,* 2008, 564.
[161] Stair & Reynolds, *Principles of Information Systems*, 306.

due to the gradual removal of trade barriers, the strengthening of global supply chains, and the arrival of customers from emerging regions.[162]

The ability to meet customers' requirements more effectively and efficiently than traditional shopping is the most significant benefit of e-commerce that has been noted in the literature. Researchers found that people who purchase online can find products with little effort, inconvenience, or time commitment. The consumer's use of the Internet for goods purchases appears to be primarily motivated by this reduced effort. Additionally, it was discovered that consumers may efficiently access and get more in-depth information on businesses, goods, and brands while simultaneously decreasing the cost and labour of information collecting. Consumers can also compare product features, availability, and costs due to this access to information, which offers some degree of anonymity. The amount of time needed to acquire information for internet buying is minimal. The next most important benefit for potential online consumers seems to be the time savings when browsing and discovering things. Consumers are encouraged to purchase online since they may choose a time that is convenient for them and is not restricted by store hours or the actual location of relevant stores.[163]

An e-commerce website can enhance customer service by using tools such as an online support desk, business websites, and e-mail. These resources allow for the low-cost resolution of many client queries and issues. In some circumstances, an e-commerce platform can offer its consumers personalised service while also customising a product or service to meet a particular customer by utilising various online technologies. By obtaining pertinent data on various customers, a certain product or service can be tailored to consumer tastes and interests.[164]

For individual customers, the advantages of m-commerce include the ability to conduct business online at any time and from any location, as well as the provision of real-time data and other helpful tools for shopping. M-commerce expedites the delivery of banking and financial services and aids in planning and communication while travelling. Finding new

[162] OECD, 'Toolkit for Protecting Digital Consumers: A Resource for G20 Policy Makers', Buenos Aires, OECD, 2018, 8.
[163] Ewelina Lacka, 'Culture Dependent Benefits of E-commerce: A Consumer Perspective' in E. Lacka et al. (eds.*), E-commerce Platform Acceptance*, Switzerland, Springer International Publishing, 2014, 153-154.
[164] Bidgoli, *Electronic commerce*, 57-58.

acquaintances and keeping up with old ones is simple due to m-commerce, which offers multimedia enjoyment wherever you are. Additionally, m-commerce offers a variety of mobile devices for contact transactions and speeds, such as the ability to find people, get prompt responses to enquiries, and compare prices in-store or through shopping comparison websites and apps. Furthermore, m-commerce makes 'smart' applications more accessible and affordable in some nations relative to the cost of using desktop computers.[165]

The advantages for consumers are what determine s-commerce's effectiveness in the primary. One of the main benefits of s-commerce seems to be the ease with which recommendations from friends and other consumers can be obtained via social media discussion groups and product review websites. Recommendations also help build consumer confidence and trust, which in turn influences their decision to buy products and services. S-commerce allows for transactions to be balanced with the unique needs, desires, tastes, and wishes of each consumer. Consumers are offered exclusive offers, such as through messages from friends on social media, resulting in significant savings, which in turn leads to more loyal consumers and faster purchasing decisions. S-commerce fits the lifestyle of mobile devices well and encourages consumers to support other consumers, increasing customer trust in suppliers is easy for consumers via closer relationships. Additionally, s-commerce enables consumers to interact socially online and receive excellent customer service from manufacturers. Customers can learn about rich social history and significance while making purchasing decisions, and they can interact with people and businesses to which they might not otherwise have access.[166] In the world of e-commerce, it is a reality to do business around the world, 7 days a week, 24 hours a day. Customers logging into a commercial website can order or purchase any product or service anywhere in the world. Holidays, weekends, non-business hours, and time zone differences are not a problem.[167]

2.3.3. Advantages to society

E-commerce benefits the welfare of society as a whole. Electronic tax refunds, public retirement, and welfare support payments can be sent safely and affordably through the

[165] Turban et al., *Electronic Commerce 2018*, 211-212.
[166] Turban et al., *Social commerce,* 14.
[167] Bidgoli, *Electronic commerce,* 56.

Internet. Additionally, e-payments may be simpler to audit and manage than check payments, providing security against fraud and theft-related losses. To the extent that communication is made by e-commerce, everyone benefits from the decrease in traffic and pollution generated by commuters. E-commerce can also make goods and services available in isolated regions.[168]

The participation of developing countries in e-commerce can accelerate economic change by giving companies and citizens access to new technologies and markets, decreasing transaction costs, and increasing efficiency by expanding information and communication networks such as the diffusion of new or improved technologies. All of these changes help raise the productivity of firms, in turn, enhance their export capacity and potentially boost their role in global value chains, and then transfer productive capital to higher-productivity activities or sectors that drive growth, income, and poverty reduction in developing countries.[169]

E-commerce is cost-efficient. Unlike a traditional environment, e-commerce does not require physical warehouse rentals, insurance, or infrastructure investments. It has changed the way companies interact with suppliers, suppliers with business partners, and customers.[170] E-commerce can assist society by raising living standards through the use of online networks to buy less expensive goods and services. E-commerce can boost homeland security by encouraging domestic security. E-commerce can also help close the digital gap by enabling people in remote and rural locations to use more services and make more meaningful purchases.[171] Finally, the expansion of e-commerce would protect the environment. This kind of growth would be more environmentally friendly and long-lasting because, due to better logistics, home delivery requires less energy than many excursions by customers. More energy can be saved during the actual creation of items that are now available as digital material.[172]

An e-commerce website should be able to maximise return on capital and investment in some circumstances as no inventory is required. In certain cases, an e-commerce platform

[168] Schneider, *Electronic Commerce,* 23.
[169] Alberto F. Lemma, 'E-commerce: The implications of current WTO negotiations for economic transformation in developing countries' *Supporting Economic Transformation,* 2017, 13.
[170] Awad, *Electronic Commerce,* 12-13.
[171] Efraim Turban et al., *Electronic Commerce: A Managerial and Social Networks Perspective,* Switzerland, Springer, 2015, 17.
[172] European Commission, 'A coherent framework for building trust in the Digital Single Market for e-commerce and online services', COM (2011), 942 final, 4.

serves as a middleman, receiving orders from customers, sending them to suppliers, and pocketing the profit. In other cases, an e-commerce platform can manage limited inventory and fulfil consumer orders via a just-in-time inventory system. The e-commerce site may avoid depreciation of inventory due to the introduction of a new product, a change in fashion or season, and also with no or little inventory.[173]

Any application of the economic activity made possible by e-commerce is genuinely significant if it improves the quality of life for people all over the world. From a societal perspective, reducing wasteful human transportation would also free up limited resources for other development efforts. More jobs will be created as a result of the emergence of new manufacturing and commercial opportunities brought on by individual requirements. The move to virtual firms will create an international division of labour while expanding foreign investment will incorporate developed countries into the global economy, promoting healthy growth. In other words, the adoption of e-commerce would advance the global system of free trade, boost economic growth, and increase the standard of living for everyone.[174]

2.3.4. Disadvantages and obstacles

E-commerce has its drawbacks despite all of its advantages. Organisations, consumers, and society are the three key actors who carry out this action. Lack of proper security, dependability, communication standards and protocols are one of the factors limiting e-commerce for businesses. There have been several allegations of software vulnerabilities as well as hacks on websites and databases. The second set of restrictions on firms is the pressure to innovate and change business models to take advantage of new opportunities, which occasionally results in company-harming initiatives. This pressure is increased and long-term competitive advantage is reduced by the ease with which business models can be copied and imitated online. Compatibility issues between ‘older’ and ‘newer’ technology provide the final constraint for companies. Some companies operate practically two different systems with no data sharing due to challenges where outdated business systems are unable to interact with web-based and Internet infrastructures.[175]

[173] Bidgoli, *Electronic commerce*, 58.
[174] Bhasker, *Electronic Commerce*, 13.
[175] Tassabehji, *Applying E-commerce in Business*, 15-16.

As e-commerce develops quickly, more and more people will take advantage of its convenience, yet it is not without issues. The most serious is the infringement on intellectual property rights and the deliberate misrepresentation that has garnered media attention as e-commerce companies compete with one another. Accessibility, confidentiality, informational integrity, and dependability are all aspects of Internet security. Most networks guarantee payment and personal information by establishing safety criteria. The usage of security servers can help to a certain extent reduce online security concerns since they employ encryption technology to stop wiretapping while online business data is being transmitted.[176]

A high level of security is necessary for e-commerce. In response to security concerns, public-key cryptography was developed, and it has revolutionised e-commerce. Due to digital signatures or certificates that allow the sender of a message or an e-commerce product to be validated, communications are now comparatively safe. Spam has become a significant financial drain on almost all businesses, leading to rules and agreements on a global scale. Important corporate identifiers known as domain names are the focus of several legal disputes and are traded for millions of dollars. Each website is often available worldwide, despite substantial regional variations in the laws governing extremism, suicide materials, malware, and censorship. The internet presents several problems, including peer-to-peer file sharing of music and video files, digital rights management, time-shifting, and format-shifting. Since e-commerce has no physical borders, it raises issues with privacy, standards, and transaction security in a global setting.[177]

E-commerce obstacles are either non-technological or technological ones. One important area that could limit some e-commerce projects is ethics. Ethical issues may lead to pressures or limitations on e-commerce company operations. However, certain ethical websites promote trust and assist online vendors.[178] Some non-technological limitations, such as worries about protection and privacy, deter customers from making purchases. The next non-technological barrier is a lack of confidence in machines, distributors, and paperless,

[176] UNIDO, 'BRICS Plus E-commerce Development Report in 2018', 19.
[177] Davidson, *The law of electronic commerce*, 1.
[178] Turban et al., *Electronic Commerce 2018,* 29.

faceless transactions that prevent purchasing and fighting change. Many legal and political issues are unsolved or unclear as a result of non-technological limitations.[179]

Regarding the kind of items that companies sell, there is also little impact on cross-border e-commerce. The results indicate that three barriers - the high cost of delivery, the restriction on suppliers selling internationally, and the expense of resolving disputes and complaints - are related to the strategic choice to conduct cross-border online transactions. The frequency of these challenges varies, though, according to the size of the business. For instance, delivery costs are more significant for larger businesses. Only smaller enterprises should be concerned with the restrictions and dispute resolution fees of suppliers. Other statistically significant barriers include the cost of taxes and product labelling for small businesses as well as copyright for microenterprises. Regarding sales, the three main factors that prevent consumers from making cross-border purchases are payment security, language proficiency, and the expense of resolving disputes and grievances. Except for dispute resolution, which has also been found to be crucial for large enterprises, these challenges are more pertinent to smaller businesses than to larger ones.[180]

2.3.5. Summary

Companies can benefit from e-commerce and realize their business strategy in the marketplace by reducing production costs, sales and distribution, strengthening the company's brand and offering better customer service. On one hand, consumers can choose from a wide range of products and services, taking advantage of the benefits of e-commerce, which will save them money, time and effort in getting the information they need. On the other hand, many people are concerned about the security of online transactions and the personal information they provide. By working together and improving the quality of communities through cutting-edge technology, the benefits of e-commerce to society can contribute to overall well-being and create a sustainable environment.

[179] Efraim Turban et al., *Introduction to Electronic Commerce and Social Commerce*, Springer, Switzerland, 2017, 24.
[180] Néstor Duch-Brown and Bertin Martens, 'Institute for Prospective Technological Studies Digital Economy Working Paper' (2015-07): Barriers to Cross-border eCommerce in the EU Digital Single Market, European Commission, *Joint Research Centre*, 2015, 33-34.

E-commerce, like two sides of the same coin, has its advantages and disadvantages. Even if these two prerequisites show the strengths and weaknesses of e-commerce transactions, other obstacles hinder and limit the effective operation of e-commerce transactions. The current e-commerce industry is known and used by all organisations, consumers, and society in general due to all these criteria and restrictions. All things considered, the benefits of e-commerce outweigh the disadvantages, as it facilitates the communication and interaction of online participants.

2.4. The classification of e-commerce transactions

Information and communication technologies are used in e-commerce to carry out market transactions between two or more parties, typically consumers and corporations. The government can occasionally be one of these parties. Although generally speaking the government is seen as a corporate agency, in some circumstances it might be considered a particular type of business with its own set of rules and regulations. E-commerce has been classified into the following groups based on the parties involved in the transaction: business-to-consumer (B2C), business-to-business (B2B), consumer-to-business (C2B), business-to-consumer (B2C), consumer-to-consumer (C2C), consumer-to-government (C2G) and business-to-government (B2G).[181] Since there are many forms of e-commerce, several methods exist to classify them. The nature of the business relationship to which the seller sells is commonly used to distinguish between different forms of e-commerce. Mobile, social, and local e-commerce can be seen as subsets of these e-commerce types.[182]

As e-commerce has grown in popularity, new improvements to business and development have occurred. The next e-commerce developments and frontiers will be consumer-to-manufacturer (C2M) and manufacturer-to-consumer (M2C). Short-circuiting the economy is a term used to describe a brand-new e-commerce model that emerged in the context of the industrial Internet and is regarded as C2M. It binds manufacturers and customers directly, removing the need for product delivery intermediaries. It achieves zero

[181] Bhasker, *Electronic commerce*, 16.
[182] Laudon & Trevor, *E-commerce*, 21-22.

commodity inventories and can satisfy customers' individualised demands by manufacturing on demand.[183]

E-commerce transactions and interactions could take on additional forms besides those already listed. Another type of e-commerce is known as Business-to-Business-to-Consumer (B2B2C), in which companies sell goods or services to clients who have their clientele. Customers of eBay, for instance, have access to a virtual marketplace. The final type of e-commerce is intra-business, which refers to all intra-organisational operations involving the exchange of products, services, or information.[184]

Since systems with different functionalities will need to be created in an organisation to accommodate transactions with buyers and suppliers, it is useful to identify opportunities for buy-side and sell-side e-commerce transactions when evaluating the strategic impact of e-commerce on an organisation. An organisation's suppliers are contacted in buy-side e-commerce transactions to obtain the resources they need. Sell-side e-commerce describes the transactions entailed in the sale of goods to clients of an organisation.[185]

A model of e-commerce known as an online-to-offline (O2O) combines online payment and customer support. O2O, a form of e-commerce, fully utilises the accessibility and speed of the electronic information network for the transmission of information. The development of O2O commerce operations exploded in 2017. The O2O business is distinguished from other forms of e-commerce, however, by its offline experience and consumption. The O2O model is consistent with previous models in its online information and money flow, which are both aspects of e-commerce along with logistics and consumption flow. However, consumers go to real storefronts for direct consumption in the O2O model, with logistics and consumer flows taking place offline, in contrast to other models where goods are delivered to consumers by express delivery. Traditional business operations can organically meld with e-commerce by fusing online and offline. O2O e-commerce is a new trend, thus it needs to be developed while taking a variety of elements into account, such as political, economic, technological, legal, and cultural aspects.[186]

---

[183] UNIDO, 'Brics Plus E-Commerce Development Report in 2018', 15-16.
[184] Radovilsky, *Business Models for E-commerce*,12-13.
[185] David Chaffey, *Digital Business and E-commerce management: Strategy, implementation and practice*, Pearson, 2015, 14.
[186] UNIDO, 'BRICS Plus E-commerce Development Report in 2018', 15.

The planned use of digital technology by business partners is referred to as collaborative commerce (c-commerce). Along the supply chain, planning, designing, researching, managing, and providing customer service to numerous partners and responsibilities are typically included. C-commerce can take place between several business partner pairs or among numerous partners who are part of a collaborative network. Collaboration through social networks and with Web 2.0 tools provides a social dimension that might enhance trust, engagement, and communication. Numerous new tools are available, some of which are being added to the established collaborative tools. Improved cooperation may enhance knowledge management, individual and organisational performance, and supply chain efficiency.[187]

Direct and indirect e-commerce are the two primary categories of e-commerce activity. Electronic ordering of actual items that still need to be physically delivered using established channels like postal services or commercial couriers is known as indirect e-commerce. Direct e-commerce involves ordering, paying for, and receiving on a worldwide scale intangible goods and services like computer software, entertainment, or information services, online. Specific opportunities are provided by both direct and indirect e-commerce. The effectiveness of the transportation infrastructure is one of several external elements that affect indirect e-commerce. Direct e-commerce fully utilises the potential of international electronic marketplaces by enabling seamless, end-to-end transactions across geographic boundaries.[188]

2.4.1. B2G and G2B transactions

Businesses sell goods and services to government agencies in B2G markets. Businesses that provide services to government entities are frequently required to adhere to additional rules or laws that control product specifications and marketing tactics. Google regularly markets its enterprise solutions to a wide range of government organisations around the world. As a result, the B2G market is a priority for corporations. Google's Search Appliance is used by many government bodies. The technology, once deployed on an agency's website, allows government officials and consumers to quickly find a wide range of papers, forms, and other

[187] Turban et al., *Electronic commerce 2018*, 161.
[188] Commission of The European Communities, 'Communication from The Commission to The Council, The European Parliament, The Economic and Social Committee and The Committee of the Regions, A European Initiative in Electronic Commerce', Brussels, 16.04.1997, COM (97) 157 final, 3.

information that has been made available online. Users may notice a difference when using the Search Appliance deployed on a government website: search results do not include paid advertisements like those found on Google.com.[189]

In B2G trades, the business is nearly always the seller and the government is almost always the buyer. In B2G, most government agencies set a low barrier (e.g., a few thousand dollars) above which all purchases must follow a contractual relationship that has been legally placed out for bid, competed for, and awarded to one or more suppliers. For the duration of the contract award, anyone in the impacted government organisation is banned from making purchases outside of the contractual bounds or from another supplier. B2G e-commerce is similar to B2B e-commerce, but there are some major differences. Many B2B features such as e-procurement, e-payments, e-collections, and e-fulfilment also apply to B2G. The key difference is that B2G e-commerce is driven not only by logistics, supply and demand, and other marketplace dynamics but also by a slew of rules and regulations that have long been applied to government procurement. Those in charge of their organisations' procurement operations adhere to processes that examine the price, quality, availability, contractual business relationships, and other items while making buy-or-not decisions in the open marketplace.[190]

B2G has typically relied on businesses reporting a big amount of information to several public entities. This data is used by government bodies to determine if enterprises comply with regulations and policies. There are two techniques to ensure compliance through reporting. The initial one is retrospective reporting, in which audits are performed after the fact, frequently by expensive auditors who manually check reports. The auditors verify that the information is correct and accurately represents the facts. The next technique is compliance by design, which makes sure that checks and controls are incorporated into system architectures and that data is gathered directly from sources without using any additional input.[191]

---

[189] E. Turban, L. Volonino & G. Wood, *Information Technology for Management Advancing Sustainable, Profitable Business Growth*, USA, Wiley, 2013, 150-160.

[190] Alan R. Simon & Steven L. Shaffer, *Data Warehousing & Business Intelligence for e-commerce,* San Francisco, Morgan Kaufmann Publishers, 2001, 107-108.

[191] N. Bharosa et al., 'Tapping into existing information flows: The transformation to compliance by design in business-to-government information exchange' *Government Information Quarterly,* vol. 30, 2013, 9–18.

Governments require information or data to make policy decisions, among other things. The more data available, the more educated decisions can be made. Some private companies in the digital economy have been hoarding vast volumes of extremely important data for policymakers. While governments do not have direct access to that data, B2G data exchange could considerably increase a government's ability to make better public policy decisions and provide more social benefit for society as a whole.[192]

Professional activities between regional, local, or federal governing bodies and businesses to meet the demands of businesses are also referred to as a G2B relationship. In a G2B interaction, transparency, participation, and collaboration are three important components. Multiple tiers of G2B operations are common, comprising multiple services and transactions that are dependent on one another. Business registration, customs, tax payment, business information provision, and public procurement are examples of typical G2B services. The European Action Plan tracks 20 different service categories, eight of which are business-related. These services are classified as follows: a) employee social contributions, b) corporation tax, c) value-added tax, d) new company registration, e) data submission to statistics offices, f) customs declarations, g) environmental permits, and h) public procurement.[193]

The G2B implementation's major goal is for the government to use electronic and technological means to meet the needs of business services. The G2B model necessitates connectivity between government agencies and corporate organisations, as well as data automation across and within enterprises, for the agency to operate efficiently. The interaction between business and government is divided into three tasks. The initial task is search-oriented when businesses can find information relevant to their industry and are related to the availability of information. Transaction-oriented is the next task in e-transactions, where the government delivers the information that businesses need. The last task is network-oriented,

[192] Bertin Martens & Nestor Duch Brown, 'The economics of business-to-government data sharing' JRC Digital Economy Working Paper, No. 2020-04, Seville, European Commission, *Joint Research Centre (JRC)*, 2020, 8.
[193] N.A. Panayiotou & V.P. Stavrou, 'Government to business e-services - A systematic literature review' *Government Information Quarterly*, vol. 38, 2021, 1-2.

where businesses can build online networks and collaborate with governments, vendors, customers, and even competitors.[194]

G2B facilitates communication between the government and various corporate entities. This allows businesses to engage in policy development and stay informed about government information such as memos, policies, rules, and laws. Businesses can take advantage of this arrangement by downloading business registration documents, applying for permits, renewing business licenses, and paying taxes. E-procurement, a government dispensation for the exchange and purchase of goods and services, is also a part of G2B. E-procurement ensures that the bidding process for government projects is transparent and free of corruption. This is only one of the numerous ways that e-government helps to reduce corruption in public service delivery systems. As a result, e-procurement allows the government to save money because there are no middlemen or agents involved in the procurement process.[195]

G2B initiatives relate to conversations and transactions between a government and a representative business that are facilitated by electronic methods. The collection of taxes and bidding on government contracts are two major ways for the government and for-profit corporations to interact. The transmission of grant requests and proposals are more common sort of engagement in the non-profit sector. In any event, these are typical instances of the types of activities that the B2G domain supports.[196]

In general, the relationship between government agencies and corporations is complicated. A lot of factors contribute to this intricacy. To begin with, there are more laws and regulations in place, as well as more points of contact than there are in the connection between government entities and citizens. Moreover, the playing field is difficult to navigate. Entrepreneurs do business with a variety of (semi)governmental entities. Consequently, public service delivery is complex and interconnected. In addition, contact moments are complicated. In some circumstances, public agencies interact with businesses in an indirect manner, such as through intermediaries. As a result, certain contacts are mediated while others

---

[194] Rian Andrian, Bayu Hendradjaya & Wikan D Sunindyo, 'Software Assessment Model Using Metrics Products for e-Government in The G2B Model' 2016 *Fourth International Conference on Information and Communication Technologies (ICoICT),* 2016, 1-2.

[195] Kelvin Joseph Bwalya & Stephen Mutula, *E-Government: Implementation, Adoption and Synthesis in Developing Countries,* Berlin, Walter de Gruyter GmbH, 2014, 29.

[196] Rhoda C. Joseph & David P. Kitlan, 'Key Issues in E-Government and Public Administration' in G. David Garson and Mehdi Khosrow-Pour, *Handbook of Research on Public Information Technology,* Hershey, Information Science Reference, 2008, 2.

are not. The business itself is the fourth and last factor of complexity. In some situations, the entrepreneur is also the corporation, whereas, in others, the entrepreneur is the accountant or bookkeeper.[197]

In the development of G2B relationships, trust and reputation are crucial. A G2B relationship built on trust and reputation can significantly reduce transaction costs for both government and business, as well as have a good social impact. Trust, on the other hand, should not be assumed; trust can be viewed as a game of cooperation with calculative qualities. Adverse selection may arise if trust-based government policy is not adequately conceived and implemented, affecting the trade environment and potentially increasing transaction costs.[198]

2.4.2. C2G and G2C transactions

Citizen participation can aid in the development and strengthening of trust between governments and citizens. This is critical to achieving excellent governance and, as a result, achieving broader economic and social objectives. The legitimacy of government actions and specific reform agendas may be called into question in the lack of trust and the rule of law. While the overall relationship is complicated, ICTs can assist citizens to participate in the policymaking process, promote transparent and responsible government, and combat corruption. At its most basic level, citizen engagement entails providing information, consulting with users, and receiving feedback. It also incorporates citizen participation in policymaking at a higher level.[199]

Despite the increasing studies, the subject of how to make effective C2G transactions' online communication remains unanswered. The complex concept of trust is one of the many conditions for making e-government and e-participation meaningful. Despite extensive research, the empirical study of trust faces various problems, which are exacerbated by the

[197] J. Jansen, L. van de Wijngaert, & W. Pieterson, 'Channel Choice and Source Choice of Entrepreneurs in a Public Organizational Context: The Dutch Case' in M.A. Wimmer et al. (Eds.): *EGOV 2010,* IFIP International Federation for Information Processing 2010, LNCS 6228, 144–155.
[198] F.A.G. den Butter et al., 'Using IT to engender trust in government-to-business relationships: The Authorized Economic Operator (AEO) as an example' *Government Information Quarterly*, vol.29, 2012, 261-274.
[199] OECD, 'The E-Government Imperative', OECD Journal on Budgeting, Paris, OECD Publishing, vol.3(1), 2003, 83.

phenomenon's multidisciplinary nature. Although trust in government and trust in Internet technology are common suspects, no clear explanation exists as to whether both are equally significant or whether there is a reversed causal relationship between e-government use and trust formation. Another key facet of trust, trust in e-government, as well as trust in e-participation, has been investigated by several experts. It is not always a covariate of trust in government or Internet technology, and it can be considered a complex phenomenon in and of itself, as recommended for e-government and e-participation.[200]

The G2C relationship refers to how the government interacts with the general public. According to recent research, governments all over the world believe that a customer-centric approach is essential for e-government success. Because of the limited availability, it may be the only area of concentration for e-government programs in places with low Internet penetration. All people who interact with the government are referred to be citizens. All electronic conversations and transactions between a government and one or more of its citizens are referred to as G2C. A 'citizen' can be a foreign person, a student, or a resident, and is often involved in one-of-a-kind contacts with the government. Governments tend to place a great emphasis on this area since serving the people is one of the founding ideals of government and governance.[201]

Whether or not a person is satisfied with the service provided by the organisation in charge of the state's driver's licensing processing, the citizen cannot simply use the Internet to find another supplier (e.g., another state) from which to obtain a driver's license. Even if citizens are dissatisfied with the municipality's high property taxes, they must pay them through a G2C website, but they cannot choose to switch to a lower-cost provider, such as a neighbouring municipality or one in a state where property taxes are extremely low. The important thing to recall is that, unlike B2C e-commerce, which is free-wheeling and eliminates all barriers, G2C e-commerce has a far more rigid set of regulations governing the relationship between the 'G' and 'C' sides. In most circumstances, citizens are limited to dealing with their particular legally binding governmental entities. Furthermore,

[200] Y. Kabanov & L. Vidiasova 'C2G Online Trust, Perceived Government Responsiveness and User Experience: A Pilot Survey in St. Petersburg, Russia' in I. Lindgren et al. (Eds.): *EGOV 2019, LNCS 11685*, IFIP International Federation for Information Processing 2019, Switzerland, Springer Nature AG, 2019, 57-68.
[201] Joseph & Kitlan, *Key Issues in E-Government and Public Administration*, 2.

governmental organisations cannot conduct business with citizens who are outside of their jurisdiction.[202]

This type of model allows the government and its citizens to communicate constructively. Citizens are allowed to use ICTs to successfully participate in governance protocols and influence policy direction. G2C applications are defined by some authors as all interactions between the government and its citizens that take place through the Internet. G2C allows appropriate citizen-government engagement and is widely regarded as an e-key of the government's purpose. The G2C model is based on information symmetry. Citizens can request basic government services such as passports, license renewals, agriculture services, marriage/birth/death certificates, government schemes, income taxes, and information on basic public services such as health care, libraries, hospital information, and education from the government. Citizens' e-participation is enabled by G2C applications, which allows for the development of e-government.[203]

The re-organisation of government is an attempt to re-establish the government-citizen relationship. Governments should treat people as customers and try to understand what they need so that citizens are more interested in and trust the government. Governments must consider how to empower citizens and allow them to take responsibility for communal and regional issues. Citizens appear to believe that only people from that area can meet the needs of that community; thus, by giving those citizens ownership of the problem and allowing them to provide feedback and suggestions to the government, citizens would see the G2C relationship as a partnership. The importance of information technology in the implementation, sustainability, and accountability of e-government is critical. It is the crucial component that connects the G2C divide, resulting in government transparency and accountability. The revealed level of change in the public agency's accountability is reflected in the level of website transparency. Citizens can examine what various departments and agencies are doing due to the ability to communicate with the government. The government's decision to limit information would demonstrate a lack of transparency and accountability.[204]

---

[202] Simon & Shaffer, *Data Warehousing & Business Intelligence for e-commerce*, 99.
[203] Bwalya & Mutula, *E-Government*, 29.
[204] Phillip R. Neely, 'The Impact and Implementation of E-Commerce in Government & Law Enforcement' *Journal of Management Policy and Practice* vol.15(1), 2014, 95-97.

2.4.3. C2C transactions

C2C e-commerce is a subset of e-commerce in which e-transactions between consumers are facilitated by a third party. Consumers buy and sell goods to each other on eBay, which is an example of a C2C e-commerce platform. The rise of C2C has resulted in a significant decrease in the usage of classified ads in newspapers to advertise and sell personal goods and services, putting a damper on that industry. C2C, on the other hand, has given many people the ability to make a living by selling items on auction websites.[205]

The Internet network's success has created a promising opportunity for the implementation of a C2C e-commerce model. Many consumers prefer the C2C model because of its benefits such as low cost and fast response time. The C2C model has more versatility than B2C models, but it also has some disadvantages. For a long time, there has been persistent competition between B2C and C2C models. The C2C model is facing unprecedented challenges, and evidence shows that low-cost and fast response times can no longer provide a competitive advantage. The C2C model's sellers must reshape their central competitiveness to compete with other methods. In today's digital industry, the most effective approach for gaining consumers is to improve service quality.[206]

Consumers may function as suppliers themselves through the Internet. C2C e-commerce relationships are those in which one consumer serves as a retailer and sells products to other consumers. Online auction sites where consumers can sell new and used goods to other consumers, are the most well-known examples of C2C experiences. Peer-to-peer interactions are described as interactions between consumers that are not commercial in nature. These interactions are completely voluntary and free of charge, just like YouTube and online music-sharing websites. Social networking sites are another form of C2C interaction. Even though these experiences are not commercial, they occur on an e-commerce platform that is brokering user-related data.[207]

---

[205] Stair & Reynolds, *Principles of Information Systems,* 302.
[206] H. Qie & J. Liu, 'The Research on the Electronic Commerce Service Quality Indicators in C2C Field' Z. Zhang et al. (eds.), *LISS 2014 Proceedings of 4th International Conference on Logistics, Informatics and Service Science,* Berlin Heidelberg, Springer-Verlag 2015, 525.
[207] Tawfik Jelassi & Francisco J. Martínez-López, *Strategies for e-Business; Concepts and Cases on value creation and digital Business transformation,* Switzerland, Springer Nature, 2020, 85.

By connecting consumers through third-party middlemen, the Internet has facilitated global C2C transactions. Online auctions or other Internet-related classified advertising could be used as intermediates. Internet intermediaries that facilitate these C2C transactions have at least two effects on economic well-being. Foremost, buyers benefit from the broader availability of things due to worldwide interconnection. There are also several online auction mechanisms. The economic and societal repercussions of these auctions are significant.[208]

C2C e-commerce is not as mature as B2B or B2C e-commerce. Because popular C2C business platforms, particularly those that leverage social media and mobile devices, are still growing, C2C e-commerce differs greatly from B2B and B2C e-commerce. Essentially, it is a platform that allows people to mobilise their talents, knowledge, and resources to produce socialised value. In the C2C industry, the firm's productive function is weakened. A company, on the other hand, can help to facilitate the production and capture of consumer value. Firms can enable every individual to produce value by providing platforms, resources, incentives, and information security. Several e-commerce models are used in C2C transactions. One of the C2C business models is an online transaction platform in which both merchants and consumers are individuals. eBay, for example, allows customers, but not corporations to sell and buy new and old stuff. Online classified platforms are another type of e-commerce model where users can find tutoring, housing, pet sales, delivery services, and other types of businesses on this type of platform. Residents are often served through ad platforms, which may offer ads or paid placements. It differs from transactional platforms in that a transaction can be made without using the platform. Since the next business model is social online platforms, consumers enjoy social connections with other consumers. Similar to an online marketplace, an online social platform might directly charge a subscription fee or take a cut of users' sales to monetise them. The next new e-commerce business model is the online crowdfunding platform that has emerged in recent years. One of the most well-known online venues for crowdfunding is Kickstarter, where those looking to launch a new venture or initiative may submit a proposal and attract investors in exchange for incentives and rewards. Clients who support initiatives on the website receive intangible social benefits as well as monetary rewards, sometimes to the point where projects become real, viable businesses. Individuals need a specific strategy and objective to explain their ideas clearly and

[208] OECD, 'OECD Internet Economy Outlook 2012', Paris, OECD Publishing, 2012, 289-290.

compellingly to differentiate themselves from the crowd. Posting an idea on one of these online crowdfunding sites alone won't get someone funded.[209]

Mobile devices provide a one-of-a-kind potential for C2C e-commerce. Many people use C2C e-commerce to get products at a lower cost, to get products that are regarded as scarce, or to sell stuff as a secondary source of income, to mention a few reasons. However, these same people have jobs and other obligations that may limit their ability to use C2C e-commerce regularly, especially when online auctions stop during business hours. As a result, mobile devices allow users to track online items at any time. Mobile devices allow users to complete transactions anytime, anywhere. C2C e-commerce has a specific user demographic: young people use it more than people of other age groups.[210]

There is also another type of e-commerce transaction such as C2B transactions, where people sell items or services to businesses through e-commerce platforms, for example when a consumer publishes online surveys for a firm to use. Another example is when a company uses crowdsourcing to encourage customers to provide services for a charge, such as contributing to a website.[211] The C2B relationship is the relationship category, in which consumers provide businesses with details about their interactions with goods or services. Book reviews on Amazon.com and user reviews on Airbnb are examples of C2B experiences. Market knowledge is then exchanged with other consumers to assist them in making more informed buying decisions. In addition, metadata of real user activity helps businesses to cater to individual requirements. Amazon.com, for example, uses shared metadata and algorithm filtering to recommend specific books to customers based on the purchase and viewing habits of other users.[212]

2.4.4. Mobile Commerce

The electronic style of conducting business and trade underwent a significant transformation over the years. A growing number of consumers now use mobile devices to

[209] Jelassi & Lopez, *Strategies for e-Business*, 161.
[210] Lori N. K. Leonard, 'C2C Mobile Commerce: Acceptance Factors', In Lee (ed) *Encyclopaedia of E-Business Development and Management in the Global Economy*, IGI Global, 2010, 759-763.
[211] Hossein Bidgoli, *MIS8*, Cengage learning Inc., USA, 2018, 180.
[212] Jelassi & Lopez, *Strategies for e-Business*, 85.

access the internet.[213] Mobile users can access any service at any time and from any location due to the widespread use of mobile devices, provided with a reliable, persistent Internet connection. Three factors - ubiquity, real-time service, and availability - can be used to summarise the value of mobile communications. These distinctive features enable mobile users to take advantage of a wide range of enhanced mobile multimedia services, as well as promote service providers and e-commerce owners to profit and generate revenue from new technologies and online platforms. Mobile devices carry personal information and preferences, making it simple to get in touch with potential customers or make buy suggestions.[214]

The first mobile transaction recorded on the market was a payment sent to two vending machines in Helsinki in 1997 via SMS. Since then, market analysts and commentators have been forecasting that m-commerce is poised to become 'the next big thing' in advertising and the selling of consumer products. M-commerce is a type of e-commerce that uses mobile devices to conduct e-transactions over public or private wireless networks, corporate intranets, or the Internet. M-commerce presents a chance to bring new products to existing clients and entice new ones to e-commerce at any time and from any location. Mobile retailing is the practice of promoting, enhancing, and adding value to the in-store buying experience through the use of mobile technology. Additionally, there is mobile marketing, which entails a range of actions taken by businesses to engage, talk to, and interact with customers via wireless, handheld devices via telecommunications networks like Wi-Fi.[215]

It is feasible to summarise the differences between e-commerce conducted online and on mobile devices into two categories: technology and value. The perceived difference in the communication network and end-user devices between m-commerce and e-commerce is related to the perceived technological gap between them. In the case of e-commerce over the Internet, end-users typically use large-screen PCs with high-definition audio and video, conventional keyboards, and suitable power supplies. In the case of m-commerce, the user interfaces consist of a small screen, a limited text input keyboard, and a small power supply.

---

[213] WTO, 'E-commerce in Developing Countries Opportunities and challenges for small and medium-sized enterprises', Geneva: World Trade Organisation, 2013, 2.
[214] Stoica Eduard & Brote Ioan Victor, 'New technologies shaping the e-commerce environment, Marketing, commerce and Tourism and a New Paradigm of Change' Revista Economica, Suplimen nr.3/2012, 383.
[215] Efraim Turban et al., *Information Technology for Management: Advancing Sustainable, Profitable Business Growth,* US, Wiley, 2013, 199.

In addition, compared to high-speed broadband networks used for e-commerce, the communication network used for m-commerce has a lesser bandwidth and a slower transmission speed.[216]

Some of the current e-commerce services can be successfully adapted to the contemporary mobile environment due to the unique qualities of the mobile services. These specific characteristics include ubiquity, which is the benefit of a mobile device being accessible at all times and locations, providing the requirement for connectivity and real-time information regardless of the user's location. The next attribute is reachability, which indicates that if a user has a mobile device, they may be promptly contacted at any time. The following feature is convenience, which refers to how easily a user can operate a smartphone in a mobile setting without turning on a computer or placing a phone call. Additionally, instant connectivity describes a mobile device's capability to swiftly and effortlessly connect to wireless networks, intranets, other devices, and the Internet. The final approach is context-sensitiveness, which is the capability of mobile applications to recognise and adjust context - the information relating to human-computer interaction - to deliver specialised, regional, and typically purpose-appropriate services.[217]

A wide range of activities involving exchanges of money is included in m-commerce. These transactions are carried out via a mobile phone. These transactions might entail both tangible and intangible items. Examples of intangible products are applications and information sent in digital format to a mobile device. Tangible products are those bought but shipped separately using a cell phone. Mobile phones can be used for a wide range of mobile transactions, including local and remote purchases at points of sale and across wireless mobile networks.[218]

2.4.5. Social commerce

[216] Y.Z. Cao et al., 'The effects of differences between E-commerce and M-commerce on the consumers' usage transfer from online to mobile channel' *International Journal of Mobile Communications*, 2015, 54.
[217] P. Benau & V. Bitos, 'Developing Mobile Commerce Applications' in Wen-Chen Hu (ed*) Selected Readings on Electronic Commerce Technologies: Contemporary Applications,* Information Science Reference, Hershey, 2009, 74-75.
[218] Y.F. Chang et al., 'Smart phone for mobile commerce' *Computer Standards & Interfaces*, vol.31, 2009, 740–747.

The introduction of social media has significantly altered the online landscape. Social media makes it easier for people to stay in touch with one another. More and more people are exchanging information on a 'many-to-many' worldwide platform that enables users to learn about the experiences of persons living in different nations. Consumers utilise social media to locate reviews of specific goods and services since they are more likely to accept peer opinions than those of traditional advertising. Social media is appealing to a sizable audience, so businesses may utilise it as a platform to expand their online presence and find new customers. Additionally, several social networking platforms now include commercial features that help businesses build client relationships and improve the marketing of their goods and services.[219]

Increased consumer interest in purchasing goods through social media, based on the opinions and recommendations of other customers, friends, and family, is also considered to be a possible driver of future e-commerce growth. Consumers today frequently perceive social media evaluations and ratings as more honest and trustworthy than conventional advertising. As a result, businesses perceive this customer feedback and evaluations as important revenue generators that help them retain their current clientele and maybe reach a wider audience. Brands and online merchants are increasingly using social media as a platform to sell their products directly, promote their products and get feedback from current or potential customers.[220]

In 2005, Yahoo initially used the term 'social commerce.' Users first associated this term with services like swapping shopping lists or reviewing specific items. Social networks, or other socially oriented platforms that are used for business transactions are known as e-commerce. Furthermore, s-commerce does not always have to result in the sale of goods; rather, it might only foster word-of-mouth through one or more social network services. The biggest change in s-commerce is the alteration in the dynamic but also sharing the experiences with others. In other words, consumers create and disseminate knowledge on their own, which

[219] International Trade Centre, 'Bringing SMEs onto the e-Commerce Highway', ITC, Geneva, 2016, 11.
[220] OECD, 'The Internet Economy on the Rise: Progress since the Seoul Declaration', Paris, OECD Publishing, 2013, 125.

has a big impact on how much goods and services are sold. By spreading information on social media in real-time, businesses can get the most out of word-of-mouth at a low cost.[221]

S-commerce refers to e-commerce transactions carried out through social media. It consists mostly of a blend of social media content, e-commerce, and e-marketing. The combination of e-commerce and e-marketing using Web 2.0 social media applications has been found to generate s-commerce. This combination is supported by ideas like social psychology, consumer behaviour, social capital, and online collaboration, and it produces several practical applications for driving s-commerce. The development and explosive expansion of mobile computing and smartphones has also aided s-commerce. M-commerce is the framework for models of s-commerce, such as location-based applications, virtual communities, virtual worlds, and networking for consumers/companies. S-commerce was made possible by advancements in marketing, technology, customers, and management, just as they had facilitated the expansion of e-commerce.[222]

As an emerging form of e-commerce, s-commerce encourages consumers to shop online and make purchases. The effective transmission of product information is a crucial element of social exchange. Therefore, marketers must comprehend how information is shared on social commerce networks. E-commerce, social media and social events are the components that make up the s-commerce domain. The phenomenon of s-commerce is complicated since it calls for knowledge in a variety of fields, including marketing tactics, algorithm design, and sociological models.[223]

S-commerce comes in two types. The first category consists of websites that enable user-generated content and employ Web 2.0 capabilities. This type restricts user interactions as it does not allow users to tag other users or send them private messages. The next category includes social network services with e-commerce features. By encouraging users to share more of their knowledge and expertise as well as their original content, these s-commerce platforms give users ways to socially interact with others and boost their preferences.[224]

---

[221] J. W. Sohn & J. K. Kim, 'Factors that influence purchase intentions in social commerce' *Technology in Society*, vol.63, 2020, 1-2.
[222] Turban et al., *Social commerce*, 8.
[223] Hui Li & Narisa Zhao, 'Better Earlier than Longer: First-Mover Advantage in Social Commerce Product' *Information Competition, Sustainability*, vol.11, 2019, 1-2.
[224] R. S. Algharabat et al., 'Investigating the Impact of Social Media Commerce Constructs on Social Trust and Customer Value Co-creation: A Theoretical Analysis' in N. P. Rana et al. (eds.), *Digital and Social Media Marketing, Advances in Theory and Practice of Emerging Markets,* Switzerland, Springer Nature AG, 2020, 43.

These are several characteristics of s-commerce that are driving its growth. One of them is the newsfeed, which social media users find on their home pages and is a stream of updates from friends and advertisers. The term 'timelines' is also used in s-commerce and it refers to a collection of historical photos and events that form a user's history and may be shared with peers. The next aspect of s-commerce is social sign-up websites, which let customers register for their websites using their social media profiles. This enables websites to obtain useful data from their social profiles for use in the marketing campaigns. Customers can share their buying experiences through browsing products, chatting online, or texting, and friends can discuss goods and services online in a collaborative purchasing environment. Network notification is also utilised in s-commerce, a setting where users can share with friends whether they like or dislike certain goods, services, or information as well as their location.[225]

The differences between e-commerce and s-commerce can be highlighted in terms of business objectives, consumer connections, and system engagement. In terms of business goals, e-commerce aims to maximise efficiency through techniques for advanced searches, one-click orders, virtual catalogues that are guided by requirements, and recommendations based on previous consumer purchases. However, s-commerce places a secondary emphasis on purchase and is geared more towards social activities like networking, communication, and knowledge exchange. In terms of system interaction, e-commerce typically provides one-way surfing, in which client data is rarely (if ever) communicated back to businesses or other users. S-commerce, on the other hand, fosters more social and cooperative methods that let customers express themselves and share their knowledge with other customers and businesses.[226]

2.4.6. Local commerce

[225] Kenneth C. Laudon & Jane P. Laudon, *Management Information Systems: Managing the digital firms*, New York, Pearson Education Ic, 2018, 423.
[226] Z. Huang & M. Benyoucef, 'From e-commerce to social commerce: A close look at design features' *Electronic Commerce Research and Applications,* vol. 12, 2013, 246-259.

Local e-commerce, as its name suggests, is a subset of e-commerce where customers are chosen depending on where they are right now. Local retailers employ a variety of online marketing techniques to draw customers to their stores.[227]

Location-based commerce (L-commerce) or LBC is the use of location-finding systems, such as GPS-enabled devices or comparable technologies (such as triangulation radios or cellular locations), to locate a customer's mobile device or gadget and deliver the appropriate services, like advertising or vehicle route optimisation. L-commerce encompasses context-aware computer technologies. It provides customers with current and relevant sales information, the chance to interact with friends, safety features (such as emergency assistance), and convenience through online shopping (the user can find out which object is nearby without going to the catalogue or the map). Customers' requests can be promoted, delivered, or fulfilled in real-time by sellers. L-commerce is essentially the delivery of m-commerce transactions to consumers who are in a certain location at a specific time. Location-aware systems are frequently used to describe location-based systems. These days, they mostly involve mobile devices like smartphones and tablets that have location-tracking capabilities, allowing various applications to use location data for social and commercial purposes. L-commerce is infrastructure-based, but its parts are based on the applications. However, there are a few requirements that are typically present in l-commerce, one of which is the location-finding component (positioning) of a GPS or other piece of equipment. There must be a mobile positioning centre, which includes a server that manages location data gathered by a location finder. Users in these transactions can be either people or objects, like cars. As for mobile devices, for instance, smartphones must include a GPS or other capability that allows the user to locate something or someone's location. The mobile communication network, which is the network that routes user requests to service providers and subsequently routes the response to the user, is also necessary for l-commerce. In l-commerce, the customers' requests must be fulfilled by service or application providers. There are also data or content providers that service providers normally need to collect to respond to requests. Additionally, the geographical information system (GIS), which uses maps and locations of

[227] Laudon & Traver, *E-commerce*, 26.

businesses, is also used. The final programme is an opt-in application, which is utilised with the user's permission (opt-in) and requires an additional piece of software.[228]

2.4.7. Summary

E-commerce, as can be seen, can be divided into a variety of categories depending on the features of the technology, the participants' types, the number of communication interactions, and the business value chains. M-commerce, a type of e-commerce that sees a higher utilisation rate, is when online business transactions are carried out on portable devices or mobile phones using wireless network systems. A mix of social networking services, Web 2.0 technology and e-commerce, as well as buying, selling, sharing information, and connecting via social media can be referred to as s-commerce. Local or location-based commerce is a type of economic activity where consumers can receive unique, personalised goods and services depending on their location and GPS technology can be used to establish their location. By classifying e-commerce, it is possible to highlight the distinctive features and similarities between the classified groups, which will help in the study of the entire e-commerce system.

[228] Turban et al., *Electronic commerce 2018,* 227.

Chapter 3. The concept of vulnerable individuals in the consumer protection law

This chapter is going to begin by looking at the two main categories of e-commerce in terms of volume and quantity, especially business-to-consumer and business-to-business transactions. After a brief overview of the EU regulatory framework in the field of consumer protection, the notion of average consumers will be revised. Later the concept of vulnerability and vulnerable consumers will be discussed in detail in terms of its definition and provisions in the EU consumer protection law to find out whether EU consumer law can properly identify and protect vulnerable individuals in online transactions.

3.1. Business-to-consumer transactions

The Internet has revolutionised the way companies do business by providing sellers and buyers with a powerful communication channel and allowing two parties to unite on e-marketplaces. B2C e-commerce is growing in popularity as more people realise its ease and capacity to respond quickly to requests, as well as when more products or services become available. An increasing number of businesses are seeing the benefits of this trend. As a result, e-commerce is becoming increasingly crucial in our daily lives. The notion of B2C is similar to traditional commerce, with the key distinction being the medium utilised to do business, which is the Internet.[229]

Conducting the B2C e-commerce cycle involves five main activities. The first activity is information sharing. A B2C e-commerce business can exchange information with its consumers through several channels, including company Web pages, online catalogues, e-mail, online advertising, video conferencing, message boards, and newsgroups. Then comes the ordering by which consumers may order goods from a B2C platform using electronic forms or e-mail. The third activity is payment, and all credit cards, e-checks and e-wallets are among the payment solutions available to consumers. The next activity is fulfilment with aim of how goods or services are distributed to consumers varies depending on whether they are physical (books, images, CDs) or digital (software, music, electronic documents). Physical

[229] C. C. Huang et al., 'The agent-based negotiation process for B2C e-*commerce' Expert Systems with Applications,* vol.37, 2010, 348-359.

goods may be delivered by air, sea, or land at various costs and with various choices. Digital goods are delivered more directly, generally requiring only uploading, but they are normally checked with digital signatures. If an organisation manages its fulfilment operations or outsources them also affects fulfilment. Delivery address verification and automated warehousing, which keeps digital items on storage media before they're shipped, are common parts of fulfilment. The last activity consists of service and support. Since e-commerce businesses do not have a physical location to help retain existing consumers, service and support are much more relevant in e-commerce than in traditional commerce. E-commerce companies can make an effort to enhance customer service and support by using any of the following methods as mail confirmations and product alerts, online surveys, help desks, and assured safe transactions since retaining existing customers is less costly than attracting new customers.[230]

B2C e-commerce is classified as pure or direct, partial or indirect, depending on how goods are delivered to customers. Pure e-commerce refers to goods that can be sold directly to customers over the Internet without the need for third-party intermediaries. Both goods with a digital format and digital services fall under this category. Other goods, such as natural ones, that do not require third-party mediation are classified as partial e-commerce. B2C e-commerce has a range of benefits for both the business and the consumer. The reduction in the business's administrative and operating costs is extremely important. The company lowers the cost of marketing by lowering the costs of producing, processing, distributing, storing, and reprinting content. Furthermore, it allows businesses to increase their market share in both domestic and foreign markets. Another significant benefit achieved by e-commerce businesses is increased price competition as a result of the absence of traditional trade intermediaries (wholesalers, distributors and retailers).[231]

The majority of social media research and success stories focus on B2C scenarios in which social media increases brand knowledge, loyalty, engagement, and sales. The ability of social media technologies to improve cooperation, increase content sharing, and develop community has been recognised. As a result, consumers and businesses are increasingly using

[230] Bidgoli, *MIS8*, 181-182.
[231] D. K. Nasiopoulos et al., 'Modeling of B2C Communication Strategies in Electronic Commerce' in A. Kavoura et al. (eds.*), Strategic Innovative Marketing, Springer Proceedings in Business and Economics*, Switzerland, Springer International Publishing, 2017, 532.

social media sites like Facebook, YouTube, LinkedIn, Pinterest, and Twitter. Marketers may raise brand exposure, generate leads and income, cultivate relationships, and build brand loyalty by tweeting to their followers.[232]

One of the characteristics of B2C e-commerce is that it takes place in a virtual world and that merchants and consumers are sometimes far apart in different countries. This reality exposes customers to greater risks and uncertainty in terms of contract violations than they would in conventional face-to-face transactions with traders based in the same jurisdiction. Modern communication creates some difficult-to-regulate problems in electronic relationships, such as sending ambiguous messages, using personal data, enforcing rules over long distances, and so on. Consumers, according to numerous studies, have a low level of trust in B2C e-commerce and are frequently hesitant to engage in such transactions due to a variety of concerns about these critical issues. The growth of B2C e-commerce appears to be limited as many consumers view online transactions as risky and are cautious when shopping online, especially in international sales.[233]

One of several attributes that embrace B2C Internet consumers is the expansion of consumer initiatives. Consumers are rational, and the influence of advertisements on web consumption is minimal. When consumers feel compelled to purchase something, they often turn to the Internet for information. They gather product-related information, analyse and compare it, and then place last-minute orders to purchase. Consumers are confronted with a market with extremely rich goods, which is also a market with tremendously updated speed, the reliability, and loyalty of consumers are seen at a lower level as network times shift so quickly. The pursuit of convenience and efficiency is another key attribute of the features of B2C consumers. The key feature of web usage is the lack of time and space constraints, enabling customers to get what they want from the comfort of their own homes. People are seeking a clear and easy website, a quick and convenient buying process, as well as a timely and rapid delivery while they go online shopping due to the increasing pace of life in modern society. The next attribute is the desire for a low price while maintaining high quality. The Internet saves businesses a lot of money on exhibition and distribution costs, resulting in

[232] K. Swani et al., 'Should tweets differ for B2B and B2C? An analysis of Fortune 500 companies' Twitter communications' Industrial Marketing Management, vol.43, 2014, 873-881.
[233] S. Yuthayotin, *Access to Justice in Transnational B2C E-Commerce A Multidimensional Analysis of Consumer Protection Mechanisms*, Switzerland, Springer, 2015, 1-2.

products priced marginally lower in the web market than in the conventional market, which is appealing to consumers in terms of e-commerce. In the online market, the cost for consumers to compare prices can almost be ignored; as a result, consumer sensitivity to price tends to be comparatively higher. The last attribute that is emphasised is the importance of the shopping experience. From the moment consumers open an e-commerce website to the moment they successfully purchase something, consumers must engage in a sequence of activities, during which any discomfort or disappointment will result in customer loss.[234]

The electronic market is the most commonplace for e-commerce transactions to take place. An e-marketplace, also known as an e-market, virtual market, or market space, is an electronic place where sellers and buyers meet and perform various types of transactions. Consumers get goods and services in exchange for money or other goods and services if bartering is used. E-markets perform the same functions as physical markets, however, computerised systems aim to make e-markets even more efficient by offering more up-to-date information and various support services, such as fast and smooth transaction execution.[235]

According to Ecommerce Europe, the organisation representing the voice of the EU e-commerce industry contributed that there is no single definition that encompasses the variety of online platforms important for this study, as well as the distinctions between online marketplaces, online shopping malls, comparison tools, search engines, and intermediaries. According to Ecommerce Europe, the term 'online platforms,' as it applies to the study, can encompass five distinct types of online platform services. The foremost platform services are the marketplaces which are digital online platforms that enable the selling consumer and/or business to deliver, advertise, and interact on the sale of their goods, services, and/or digital content directly to other consumers or traders who are interested in purchasing these products, services, and/or digital content under their name, risk, and liability. Shopping malls are the following form of digital online platforms that enable companies to display and operate an online store on the platform. Intermediaries/brokers are the next types of digital online channels that link sellers and buyers/offer and demand as a basic service. There are also search engines which are interactive web platforms that enable interested parties, whether customers

[234] Q. Zhang 'Customer Satisfaction in B2C E-Commerce Market' in W. Du (ed.), *Informatics and Management Science VI, Lecture Notes in Electrical Engineering 209*, London, Springer-Verlag, 2013, 283-284.
[235] Efraim Turban et al., *E-commerce: A managerial and social networks perspective*, Switzerland, Springer, 2017, 57.

or experts, to search for and locate goods, services, and/or digital content from various sellers or providers. The final form is the comparison tools which are digital online platforms that allow interested parties, whether consumers or professionals, to compare goods, services, and/or digital content from different vendors based on one or more criteria such as price, quality, time, functionality, or user reviews.[236]

Online marketplaces are spreading at an unprecedented rate, and the number of transactions on them is increasing. One clear reason for this new trend is that online shoppers prefer to shop at e-marketplaces rather than digital storefronts because of the lower purchasing costs associated with the option to compare numerous sellers. Unfortunately, the number of fraud and other forms of victimisation in e-marketplaces has also increased. E-marketplaces are particularly sensitive to cyber threats arising from online transactions. This is mostly since the e-marketplace business model comprises an intermediary that connects vendors and buyers, and intermediates are not liable for the sellers' sales transactions.[237]

Many researchers tried to figure out why consumers do not trust online sales. Most consumers believe that there is a high likelihood of opportunistic conduct in online purchases, according to research. The sophisticated technology of the internet creates a conducive atmosphere for the practice of providing incorrect or misleading information as well as for outright fraud, particularly when it comes to payment and privacy in online transactions. Additionally, especially in the cross-border market, websites or online stores can be created with little effort and without any obvious regulatory oversight. Traders who engage in unethical behaviour may emerge and vanish without warning. Due to the lack of physical touch and the vast distance between vendors and buyers, there is a chance that products and services will be misrepresented and won't be delivered once payment has been completed. When that occurs, consumers will experience a situation that is more challenging and complicated than in the case of conventional sales. In an electronic network, it is difficult for consumers to keep track of merchants who are not physically near them. It can also be exceedingly difficult and expensive to find business operators whose locations are difficult to

[236] E-commerce Europe, 'Policy recommendations on the role of online platforms in the e-commerce sector', Brussels, 2016, 3-6.
[237] I.B. Hong & H. Cho, 'The impact of consumer trust on attitudinal loyalty and purchase intentions in B2C e-marketplaces: Intermediary trust vs. seller trust' *International Journal of Information Management,* vol.31, 2011, 469-479.

identify and figure out where and how consumers might seek remedy. The aforementioned elements, which stem from the unique characteristics of the online market, are situations that lower consumer confidence. The belief among many consumers today that online transactions are likely to involve opportunistic conduct, which undermines consumer confidence, appears to be one issue limiting the potential expansion of B2C e-transactions. To increase consumer willingness to make online transactions, it is required to alter this mentality. Modern nations have taken an interest in this topic since it tends to increase consumer confidence in B2C e-transactions.[238]

Consumers have benefited greatly from the rapid expansion of B2C e-commerce, which has simplified their search for product information and improved the quality of their online purchasing decisions. However, there is evidence that the lack of crucial information is deterring consumers from making purchases. That is, the information offered by e-vendors does not always meet the information needs of online consumers. Consumer-required information is sometimes unavailable, and in certain cases, e-vendors purposefully fail to offer it, resulting in a lack of information transparency.[239]

3.1.1. Regulation of B2C transactions

Although the original reference to consumer protection was in the Treaty of Rome under the common agricultural Policy (Art.39)[240], there was no proposal to further create a consumer protection law as part of Community legislation. With the establishment of the TFEU, the guidelines in the field of consumer protection have changed for the better, since the requirements of consumer protection should be taken into account when defining and implementing other policies and measures of the Union (Art.12)[241]. According to Art. 38 of the EU Charter 'Union policies shall ensure a high level of consumer protection.'[242] With

[238] Yuthayotin, *Access to Justice in Transnational B2C E-Commerce*, 24-25.
[239] L. Zhou et al., 'Perceived information transparency in B2C e-commerce: An empirical investigation' *Information and Management*, vol.55, 2018, pp. 912-927.
[240] European Union, Treaty Establishing the European Community (Consolidated Version), Rome Treaty, 25 March 1957, Art.39.
[241] TFEU, Art.12.
[242] Charter of Fundamental Rights of the European Union OJ C 326, 26.10.2012, p. 391–407, Art.38.

subsequent initiatives like the Review of Consumer Acquis[243], REFIT[244], Fitness Check[245], New Deal for Consumer[246], New Consumer Agenda[247], and the latest in progress, Digital Fairness-Fitness Check on Consumer Law[248] which is expected to be completed by 2024, the EU has attempted to strengthen the law on consumer protection. These efforts demonstrate the EU's desire to fully harmonise and enforce consumer protection.

EU has a legal personality both as a legal entity and as an international organisation and as a decision-making body and as a union of MSs, but none of this detracts from the EU's ability to regulate online commercial relations between businesses and consumers. That's why as the main regulatory base for B2C transactions, the main objective, scope, and interpretation of Directive 98/6/EC, Directive 2005/29/EC and Directive 2009/22/EC will be emphasized.

3.1.1.1. Indication of the prices of products offered to consumers

The most effective approach to allow consumers to assess and compare product pricing, so they could make informed decisions based on straightforward comparisons, was to display the selling price and unit price. As a result, the EU legislators passed Directive 98/6/EC on consumer protection in the price indication of products offered to consumers (PID). The goal of this Directive was to make it mandatory for traders to display the selling price and the price per unit of measurement of products they sell to consumers to improve consumer knowledge and make price comparisons easier. The selling price and unit price must be unambiguous, immediately recognisable, and legible. The final price for a unit of the product, or a certain

[243] European Commission, 'Green paper on the Review of the Consumer Acquis', OJC 61, 15.3.2007, 1–23.
[244] European Commission, 'Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions Smart Regulation in the European Union', Brussels, 8.10.2010 COM (2010) 543 final, 1-12.
[245] European Commission, 'Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions EU Regulatory Fitness', Strasbourg, 12.12.2012, COM (2012) 746 final, 1-11.
[246] European Commission, 'Communication from The Commission to The European Parliament, The Council and The European Economic and Social Committee A New Deal for Consumers', COM/2018/0183 final, 1.
[247] European Commission, 'Communication from The Commission to The European Parliament and The Council New Consumer Agenda Strengthening consumer resilience for sustainable recovery', COM/2020/696 final, 1-2.
[248] Digital fairness - fitness check on EU consumer law <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_enlast> accessed 23 Aug. 2023

quantity of the product, including VAT and all other taxes, was the selling price for this Directive. This Directive repealed Directives 79/581/EEC (foodstuff prices) and 88/314/EEC (non-food product prices) with effect from March 18, 2000.[249]

The PID's scope of application was confined to products, that's why it did not apply to services. Despite the absence of a definition in this Directive, the term 'products' might be understood in light of other rules of the acquis as encompassing any movable items. According to the Commission's assessment announced in 2006, there was widespread agreement that the PID had helped to strengthen consumers' economic interests, while the exact amount of its influence was unknown. When it came to formulating its transposition measures, the PID gave the MS a lot of leeway. Several articles introduced open regulatory alternatives for national lawmakers, resulting in significant differences in national laws implementing PID in various areas.[250]

The Directive (EU) 2019/2161 on the better enforcement and modernisation of Union consumer protection rules amended Directive 98/6/EC as it required guiding criteria for penalties. The required amendment was the insertion of Art.6a which stated that any price reduction announcement must have included the previous price imposed by the trader for a certain amount of time before the price reduction. The 'prior price' referred to the trader's lowest price for some time not less than 30 days before the execution of the price reduction. Various restrictions might apply to items that were likely to deteriorate or expire quickly in the different MS.' Art.8 specified that the MS must have established procedures for enforcing national legislation enacted under this Directive, as well as take all necessary steps to ensure that they were implemented. The punishments imposed had to be effective, proportionate, and deterrent. By November 28, 2021, MS had to notify the Commission of the referred rules and measures, as well as any subsequent amendments affecting them.[251]

Art.6a addresses the issue of price reduction transparency by establishing explicit procedures to verify that they are legitimate. Art.6a aims to prevent traders from raising the

[249] Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of the prices of products offered to consumers OJ L 80, 18.3.1998, 27-31.
[250] European Commission, 'Communication from The Commission to The Council and The European Parliament on the implementation of Directive 1998/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of prices of products offered to consumers', Brussels, 21.6.2006 COM (2006) 325 final, 6.
[251] Directive (EU) 2019/2161, OJ L 328, 7–28.

reference price unnecessarily and/or deceiving consumers about the discount amount. It improves transparency and assures that when a price drop is advertised, consumers pay less for the goods. The new clause on price reductions also makes it easier for enforcement and market surveillance agencies to monitor the fairness of price reductions since it establishes explicit guidelines for the reference 'prior' price on which the stated reduction must be based.[252]

In *Commission v. Belgium case* (C-421/12), the Court emphasized the role of the Directive, stating that 'It should be remembered, however, that, as observed by the Advocate General in point 58 et seq. of his Opinion, the purpose of Directive 98/6 is not to protect consumers concerning the indication of prices, in general, or concerning the economic reality of announcements of price reductions, but specifically about the indication of the prices of products by reference to different units of quantity.'[253] Since the Directive only dealt with the indication of prices of products, any services or any digital content was excluded from its scope.

So, to improve consumer knowledge and facilitate price comparisons, Directive 98/6/EC mandated that the selling price and the unit price of any product sold by traders to consumers must be specified. A new provision addressing notifying consumers of price reductions was added to Directive 98/6/EC through the amendments made to Directive (EU) 2019/2161. Any notice of a price reduction must expressly state the previous price the trader had in place (prior price). The amendment gave MS regulatory choices with relation to products that were likely to degrade or expire quickly, particularly food, goods that had been on the market for less than 30 days, and goods that were continuously discounted in price. A set of requirements for the imposition of penalties has been added to the existing requirement that MS implement effective, appropriate, and deterrent consequences for violations of national laws on price indications.

3.1.1.2. Unfair commercial practices

[252] Commission Notice, 'Guidance on the interpretation and application of Article 6a of Directive 98/6/EC of the European Parliament and of the Council on consumer protection in the indication of the prices of products offered to consumers (Text with EEA relevance)' (2021/C 526/02), 5.
[253] *Commission v Belgium,* C-421/12, Judgment of the Court (Third Chamber), 10 July 2014, para.59.

There have been discrepancies that have made it unclear which national standards apply to unfair commercial practices that harm consumers' economic interests and created several barriers for businesses as well. As consumers were unsettled by these obstacles to their rights, the EU legislators enacted Directive 2005/29/EC on unfair business-to-consumer commercial practices in the Internal Market, also known as the 'Unfair Commercial Practices Directive' (UCPD). The UCPD harmonised MS rules against unfair commercial activities, including unfair advertising, that directly affected consumers' economic interests and, as a result, indirectly undermined legitimate rivals' economic interests. Following the concept of proportionality, the UCPD safeguarded consumers against the effects of such unfair economic practices when they were serious while acknowledging that the impact on consumers might be negligible in some situations. Consumers' economic interests were directly protected by this Directive from unfair business-to-consumer commercial practices. It excluded commercial practices that were carried out largely for other goals, such as commercial communication aimed at investors, such as annual reports and promotional brochures.[254]

The UCPD amended Directives 84/450/EEC[255], 97/7/EC[256], 98/27/EC[257] and 2002/65/EC[258] as it was important to ensure consistency between the UCPD and the Community legislation in force at that time. The UCPD has contributed to the Community acquis, which covers commercial practices detrimental to the economic interests of consumers. As a result, this Directive's single, comprehensive prohibition covered all unfair commercial activities that distorted consumers' economic behaviour. The general ban was supplemented by rules governing the two most common forms of commercial practices, namely 'misleading commercial practices' and 'aggressive commercial practices.' It was

[254] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (Text with EEA relevance) OJ L 149, 11.6.2005, 22–39.

[255] Council Directive 84/450/EEC of 10 September 1984 relating to the approximation of the laws, regulations and administrative provisions of the Member States concerning misleading advertising OJL 250, 19.9.1984, 17-20.

[256] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, OJ L 144, 4.6.1997, 19–27.

[257] Directive 98/27/EC of the European Parliament and of the Council of 19 May 1998 on injunctions for the protection of consumers' interests, OJ L 166, 11.6.1998, 51–55.

[258] Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC OJ L 271, 9.10.2002, 16–24.

desirable that misleading commercial practices, including misleading advertising, covered those practices that deceived the consumers and so hindered them from making an informed and efficient decision. The UCPD divided misleading practices into two categories: a) misleading actions and b) misleading omissions. The goal of the UCPD was to help the internal market work properly and to achieve a high degree of consumer protection by harmonising the MS' laws, regulations, and administrative rules on unfair commercial activities that damaged consumers' economic interests. According to UCPD, a 'consumer' is any natural person engaging for reasons other than his trade, business, craft, or profession in commercial practices covered by this Directive. 'Trader' referred to any natural or legal person operating in the name of or on behalf of a trader in commercial practices covered by this Directive for reasons relating to his trade, business, craft, or profession. Any commodities or service, including immovable property, rights, and liabilities, is referred to as a 'product.' Any act, omission, course of conduct or representation, commercial communication including advertising and marketing, by a trader, directly linked with the promotion, sale, or supply of a product to consumers is referred to as 'business-to-consumer commercial practices.' This Directive applied to unfair business-to-consumer commercial activities, as defined in Art.5, before, during, and after a product-related commercial transaction.[259]

To guide key concepts and provisions of the UCPD that were considered problematic, in 2009 the Commission published Guidance[260] on the Implementation of UCPD. Later, the First Report provided a first review of the application and an evaluation of UCPD in the MS. This Report relied on data collected on behalf of the Commission during a study performed in 2011/2012 to assess this Directive's application in the domains of financial services and real estate.[261]

The guidance on the implementation and application of the UCPD which was released in 2016 aimed to simplify the execution of the UCPD. This guidance was based on section 6

[259] Directive 2005/29/, OJ L 149, Art.2.
[260] European Commission, 'Commission Staff Working Document Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices', Brussels, 4.12.2009 SEC (2009) 1666 final, 1.
[261] European Commission, 'Report From The Commission To The European Parliament, The Council And The European Economic And Social Committee First Report on the application of Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive')' Brussels, 14.3.2013 COM (2013) 139 final, 2.

of the Commission's Communication on a 'comprehensive approach to boosting cross-border e-Commerce for Europe's citizens and businesses.'[262] Any authoritative interpretation of the law should be based solely on UCPD and other relevant legal acts and principles. Only the CJEU had the authority to interpret Union legislation authoritatively. Except for the acts enumerated in Annex I to this Directive, determining whether commercial conduct was unfair under the UCPD had to be done on a case-by-case basis. The MS had the authority to make this assessment.[263]

The UCPD was the Directive that had the most difficulty being transposed out of all of the Directives covered by the Fitness Check. The Commission had launched 14 infringement charges over erroneous transposition of the UCPD following a rigorous transposition examination and multiple EU Pilot processes. The UCPD's principle-based approach, in particular, was 'future-proof' and 'technology-neutral', in that it permitted national authorities and courts to adjust their evaluations in response to the rapid development of new products, services, and selling methods. The Fitness Check discovered that the principle-based approach of UCPD only occasionally resulted in the different application of the same principles in the majority of MS and that such divergent application had no appreciable detrimental effect on cross-border commerce. Also, no notable inconsistencies were found in the substantial body of national case law on the UCPD's application that is now being compiled in preparation for the upcoming publication of a unified Consumer Law Database. The UCPD gave authorities and courts the power to fine merchants and stop their illegal behaviour, which has proven very useful in protecting consumers from misleading or aggressive marketing activities. The UCPD, on the other hand, offered no provision for individual remedies for consumers who were harmed, such as a right to declare a contract null and void as a result of unfair business practices or a right to compensation.[264]

---

[262] European Commission, 'Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions: A comprehensive approach to stimulating cross-border e-Commerce for Europe's citizens and businesses', COM/2016/0320 final, 8.
[263] European Commission, 'Commission Staff Working Document Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices Accompanying the Document Communication from The Commission to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions A comprehensive approach to stimulating cross-border e-Commerce for Europe's citizens and businesses', Brussels, 25.5.2016 SWD (2016) 163 final, 3.
[264] European Commission, 'Commission Staff Working Document Report of the Fitness Check', Brussels, 23.5.2017 SWD (2017) 209 final, 4.

The penalty rules of the UCPD, which was in place at the time, had to be updated as part of the approval of Directive (EU) 2019/2161 for better implementation and modernisation of EU consumer protection since penalties were governed differently among nations in the EU. In this regard, the UCPD should be amended to make it clear that practices in which a trader provided information to a consumer in response to the consumer's online search query without clearly disclosing any paid advertising or payment specifically to achieve a higher ranking of products within the search results should be prohibited. When a trader paid the provider of online search functionality directly or indirectly for a higher ranking of a product in the search results, the provider of online search functionality should inform consumers in a succinct, easily available, and understandable manner. However, to cover new technologies, the definition of 'online marketplace' should be modified and made more technologically neutral. Specific information requirements for online marketplaces should be provided under the UCPD to notify consumers using online marketplaces and whether they engage in a contract with a trader or a non-trader, such as another consumer.[265]

The information requirements for the invitation to purchase a product at a certain price were set out in Art.7(4) of the UPCD. Those criteria applied at the advertising stage, but Directive 2011/83/EU imposed the same and other, more thorough disclosure requirements at a later pre-contractual stage (i.e., just before the consumer enters into a contract). Therefore, information in invitations to purchase at the stage of advertising in UPCD should be deleted. The UPCD was unaffected by any requirements of establishment or authorisation regimes that the MS might impose on traders in the context of events held somewhere other than a trader's premises. One of the amendments was to expand the scope of the meaning of 'products' by adding digital services and digital content, as well as rights and obligations with the old meaning of 'products', which meant any product or service, including real estate. Ranking and online marketplace definitions were also introduced. The relative importance given to products as presented, organised, or conveyed by the trader, regardless of the technological means utilised for such presentation, organisation, or communication, was referred to as 'ranking.' A service using software, such as a website, part of a website, or an application, maintained by or on behalf of a trader that allowed consumers to enter into distance contracts with other traders or consumers was referred to as an 'online marketplace.'

[265] Directive (EU) 2019/2161, OJ L 328, 7–28.

Articles 3, 6, and 7 have all undergone changes, but other articles (like Art.11a) have subclauses added to them, and others, like Art.13 of the rules on penalties, have even been repealed by the new rules.[266]

To simplify the execution of the Directive, a new 'Commission Notice' on the interpretation and application of the UPCD' was issued in 2021. The Notice was intended to raise awareness of the UCPD among all stakeholders in the EU, including consumers, businesses, MS agencies, national courts and legal practitioners. It addresses the changes introduced by Directive (EU) 2019/2161 on better enforcement and modernisation of EU consumer protection rules, which would come into force on May 28, 2022. The UCPD also protects the economic interests of consumers through its horizontal nature and the underlying concept of full harmonisation. It offers a standard regulatory framework that harmonises national rules to remove internal market obstacles and promote legal certainty for both consumers and companies. To attain a higher level of consumer protection, MS may not introduce stronger regulations than those outlined in the Directive unless specifically authorised by the Directive, according to the UCPD. As a result, the UCPD has no bearing on MS' ability to enact rules governing business conduct for reasons of health, safety, or environmental protection.[267]

In total *Belgium case* the Court found that 'Thus, the Directive fully harmonises rules at the Community level. Accordingly, the MS may not adopt stricter rules than those provided for in the Directive, even to achieve a higher level of consumer protection. In the light of the foregoing, the Directive must be interpreted as precluding national legislation, such as that at issue in the disputes in the main proceedings, which, with certain exceptions, and without taking account of the specific circumstances, imposes a general prohibition of combined offers made by a vendor to a consumer.'[268] The concept of a 'general prohibition of combined offers' was also considered by the Court in *Telekomunikacja Polska* case (C-522/08) in its legal interpretation.[269] In *Europamur Alimentación SA* case (C-295/16) the Court established

[266] Ibid, Art.7.
[267] Commission Notice, 'Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (Text with EEA relevance)' C/2021/9320 OJ C 526, 29.12.2021, 1-129.
[268] *VTB-VAB NV v Total Belgium NV,* Joined cases C-261/07 and C-299/07, Judgment of the Court (First Chamber) of 23 April 2009, para. 52, 68.
[269] *Telekomunikacja Polska,* C-522/08, Judgment of the Court (Third Chamber) of 11 March 2010, para. 33.

that 'UCPD must be interpreted as precluding a national provision, such as that at issue in the main proceedings, which contains a general prohibition on offering for sale or selling goods at a loss and which lays down grounds of derogation from that prohibition that are based on criteria not appearing in that directive.'[270]

In the *UPC Magyarország* case (C-388/13), the Court stated that the 'UCPD must be interpreted as meaning that if a commercial practice meets all of the criteria specified in Art.6(1) of that directive for classification as a misleading practice concerning the consumer, it is not necessary further to determine whether such a practice is also contrary to the requirements of professional diligence, as referred to in Art.5(2)(a) of that directive, for it legitimately to be regarded as unfair and, consequently, prohibited following Art.5(1) of that directive.'[271] In *Canal Digital Danmark A/S* (C-611/14) the Court determined that 'Art.7(4) of Directive 2005/29 must be interpreted as meaning that it contains an exhaustive list of the material information that must be included in an invitation to purchase. The fact that a trader provides, in an invitation to purchase, all the information does not preclude that invitation from being regarded as a misleading commercial practice within the meaning of Art. 6(1) or Art. 7(2) of that directive.'[272]

So, to protect consumers' economic interests before, during, and after a commercial transaction has taken place, Directive 2005/29/EC defined the unfair business-to-consumer commercial practices that are prohibited in the EU and applied to any act or omission directly related to the promotion, sale, or supply of a product by a trader to consumers. Additionally, regardless of the location of the sale or purchase within the EU, the UCPD guaranteed all consumers the same level of protection. Concerning better enforcing and modernising EU consumer protection laws, Directive (EU) 2019/2161 revised the UCPD to take into account new market trends, particularly internet marketing.

3.1.1.3. Injunctions for the protection of consumers' interest

Since the systems for enforcing Directive 98/27/EC, both at national and at Community level, did not always allow for the timely termination of infringements affecting the collective

[270] *Europamur Alimentación,* C-295/16, Judgment of the Court (Fifth Chamber) of 19 October 2017, para. 43.
[271] *UPC Magyarország,* C-388/13, Judgment of the Court (First Chamber) of 16 April 2015, para. 63.
[272] *Canal Digital Danmark,* C-611/14, Judgment of the Court (Fifth Chamber) of 26 October 2016, para. 72.

interests of consumers, a new Directive 2009/22/EC on injunctions (ID) for protection of consumer interests has been enacted. Individual actions taken by individuals who were harmed by an infringement were unaffected since collective interests did not encompass the interests of individuals who were harmed as a result of an infringement. To protect the collective interests of consumers covered by the Directives listed in Annex I and to ensure the efficient operation of the internal market, this Directive aimed to harmonise the laws, regulations, and administrative provisions of the MS concerning actions for an injunction referred to in Art.2. Under the ID, 'an infringement' referred to any action that impaired the group interests mentioned in para.1 of Art.1 and was against the Directives specified in Annex I as transferred into the internal legal order of the MS. The MS should take the necessary steps to ensure that, in the event of an infringement coming from that MS and the interests protected by that qualified entity were impacted by the infringement, any qualified entity from another MS may apply to the court or administrative authority referred to in Art.2 upon presentation of the list stipulated in para.3 of this Article. Anybody or organisation that is lawfully created following the laws of MS and has a legitimate interest in ensuring that the provisions mentioned in Art.1 are followed is referred to as a 'qualified entity.' The MS would determine whether the party requesting the injunction had to confer with the qualifying entity. If the infringement did not stop after two weeks of receiving the consultation request, the affected party may file an injunction action without further delay.[273]

A significant advantage of the ID, according to the Commission's first ID Report from 2008, was the establishment of a process for seeking injunctions to protect consumers' collective interests across all MS. Although consumer organisations used this strategy for national violations with some degree of success, it was found that this approach for permitting eligible enterprises from one MS to operate in another MS was not as successful as anticipated.[274] In its second 2012 Report, the Commission concluded that the injunctive actions were a useful tool for defending the interests of all consumers because qualified entities were becoming more familiar with the capabilities of the ID and gaining experience

[273] Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests (Codified version) Text with EEA relevance OJ L 110, 1.5.2009, 30-36.
[274] European Commission, 'Report from The Commission concerning the application of Directive 98/27/EC of the European Parliament and of the Council on injunctions for the protection of consumers' interest', Brussels, 18.11.2008 COM (2008) 756 final, 5.

with its implementation. However, despite significant differences in its use and their untapped potential due to several shortcomings, the Commission took the final decision not to propose amendments to the ID at that time and that the situation would be reviewed when preparing the next implementation report.[275]

The Commission, with its Recommendation (2013/396/EU) concerning all situations where a violation of the rules established at the Union level may cause damage to natural and legal entities, intended to facilitate access to justice for violations of the Union law. Following this recommendation, each MS was to create a national system of collective redress that adhered to the same fundamental principles across the Union but also took into account local legal customs and protected against misuse. This recommendation aimed to ensure appropriate procedural safeguards to prevent abusive litigation while also enhancing access to justice, stopping illegal practices, and enabling wronged parties to collect compensation when rights given by the Union law were breached. Where appropriate and relevant to the particular principles, this Recommendation addressed both compensatory and injunctive collective remedies. All MS should have national collective redress mechanisms that conformed to the fundamental principles outlined in this Recommendation for both injunctive and compensating measures. These principles should be applied consistently throughout the Union while taking into account the different legal traditions of the individual MS.[276]

The results of the Lot.1 Study confirmed the Commission's reports that the injunction procedure, which has been introduced across the EU, has benefited European consumers by consistently halting infringements of consumer protection laws. Since the ID's injunctive procedure sought to prohibit infringements that jeopardized the interests of collective consumers, injunctions were a particularly effective tool for carrying out EU consumer law. The Study recommended increased harmonisation of the injunction procedure at the EU level to considerably strengthen the enforcement of EU consumer legislation given weaknesses in the effectiveness and limited efficacy findings. The 'Fitness Check' found that the ID was procedural and regulated how bodies selected by MS could act before courts or administrative

[275] European Commission, 'Report from The Commission to The European Parliament and The Council Concerning the application of Directive 2009/22/EC of the European Parliament and of the Council on injunctions for the protection of consumers' interest', Brussels, 6.11.2012 COM (2012) 635 final, 7.
[276] European Commission, 'Commission Recommendation of 11 June 2013 on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union Law', OJ L 201, 26.7.2013, 60-65.

authorities to prevent traders from breaching EU consumer law. In terms of procedural law, the ID's most evident and significant benefit for consumers was the ability to enforce essential underlying EU substantive consumer protection legislation through collective injunctive cases. When a widespread infringement occurred and individual consumers did not take legal action for a variety of reasons such as a lack of awareness of their rights, a lack of financial resources, or psychological apprehension, the collective action taken by an entity to stop the infringement and prohibit it in the future benefited all affected consumers. Individual consumers were not parties to the proceedings initiated by the entity acting to safeguard their collective interest; therefore, they suffered no costs related to the injunction action as stated by the ID.[277]

The new Directive 2020/1828 on consumer protection representation has superseded the ID because the ID did not sufficiently address concerns with consumer protection law enforcement and required significant revisions. This Directive created requirements to guarantee that all MS have access to a framework for collective consumer interest representation in representative actions and to prevent abusive litigation. This new Directive's purpose was to improve consumers' access to justice in this area by harmonising various provisions of the laws, rules, and administrative procedures governing representative actions in the MS to support the internal market's smooth operation. In areas falling within the scope of the legal acts listed in Annex I, the implementation of this Directive should not constitute grounds for compromising consumer protection. Qualified entities were free to use any procedural methods available to them under Union or national law to protect the interests of consumers collectively. This Directive covered collective actions against traders who infringe the provisions of Union law listed in Annex I, including those transposed into national law, which harms or may prejudice the collective interests of consumers. It applied to both local and cross-border infringements, as well as infringements that happened either before or after the representative action was filed. This Directive does not affect the provisions of Union or national legislation establishing contractual and non-contractual remedies available to consumers for the infringements. MS had to ensure that entities, in particular consumer organisations and those representing members from several MS, can be designated as qualified entities to bring domestic, and cross-border representative actions. By December

[277] European Commission, 'Report of the Fitness Check', SWD (2017) 209 final, 4.

26, 2023, each Member State must submit to the Commission a list of qualified entities it has designated in advance to institute cross-border representative proceedings, including the names and statutory purposes of the qualified entities. Acts of representation initiated on or after 25 June 2023 should be governed by the laws, regulations and administrative provisions transposing this Directive. Acts of representation filed before 25 June 2023 must be subject to laws, regulations and administrative provisions transposing Directive 2009/22/EC. By 25 December 2022, the MS must adopt and publish the laws, regulations and administrative measures necessary to comply with this Directive. They must notify the Commission as soon as possible and begin implementing these measures on 25 June 2023.[278]

So, the Injunctive Directive, which established EU regulations to make sure that injunctions were strong enough to end violations that were detrimental to the interests of consumers as a whole, would be repealed by Directive (EU) 2020/1828 as of June 25, 2023. Injunctions sought to stop or forbid violations that went against the general interests of consumers. These injunctions were more effective due to the legislation being aligned with this directive, which also improved the efficiency of the EU's internal market. The violations in inquiry related to consumer credit, package travel, unfair terms in consumer contracts, distance contracts, and unfair commercial practices. Annex I of Directive 2009/22/EC contained a complete list of the relevant concerns.

The protection of collective consumer interests in the EU will alter after June 25, 2023, with the implementation of the recently adopted Directive 2020/1828 on representative actions for the protection of consumer' collective interests. Through representational action, including international representational action, this new Directive empowers organisations or public authorities assigned by EU MS to seek injunctive or redress action on behalf of consumer groups. As relevant and permitted by EU or national legislation, these sectors include suing businesses that violate consumer rights concerning financial services, travel and tourism, energy, health, telecommunications, and data protection. It is up to the MS' discretion to decide whether the representative action can be brought in judicial or administrative proceedings, or both, depending on the pertinent area of law or the pertinent

[278] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (Text with EEA relevance) OJ L 409, 4.12.2020, 1-27.

economic sector. This is because both judicial and administrative procedures may effectively and efficiently serve the protection of the collective interests of consumers.

3.1.2. Summary

In overall, it is clear that the development of B2C transactions was followed by numerous ups and downs, depending on the technological environment and the cooperation of market participants with one another. As the popularity of B2C transactions shows, both businesses and consumers must cooperate for transactions to be simple and profitable. Because neither party can achieve the peak of their connection without the cooperation and the usage of cutting-edge information technology, which results in ongoing and reliable B2C transactions.

EU authorities have also attempted to protect the operating principles and functioning basis by setting adequate grounds for B2C transactions to keep these partnerships in excellent form and manner. As a result, B2C transactions have been, are, and will continue to be high on the EU agenda, as both businesses and consumers are key actors in internal markets. Another notable feature of B2C transactions is that EU authorities attempt to align and adapt previously adopted legislative frameworks with current technology standards and concerns, which is a very positive attitude toward the future growth of B2C transactions. There are many areas of interest to both businesses and consumers; but, from the standpoint of a consumer in B2C interactions, unfair commercial practises, price indication of consumer products, and injunctions for the protection of consumers' interests are more intriguing areas. All this demonstrates that B2C transactions are becoming more complex and constantly covering more and more areas, striving to effectively create and maintain consumer interest.

3.2. Business-to-business transactions

Almost every corporation in the world was discussing B2B during the late 1990s technology surge. Since the premise was sound and the possibilities were limitless, many businesses rushed to implement something, anything, to become a part of this new business transformation. While the rise of B2B e-commerce has opened up opportunities for companies

to improve their purchasing systems, increase productivity and profitability, it was not a magic solution once thought of, but rather just another useful business tool used in the right circumstances. Despite the dot.com bubble burst and the global crisis, online B2B trading exchanges are still growing. Online B2B e-marketplaces have remained resilient by offering significant advantages over offline transactions, such as cheaper prices for buyers, more access to customers for suppliers, and better transparency for all parties across the supply chain.[279]

B2B e-commerce is a subset of e-commerce in which all participants are businesses. B2B e-commerce is a valuable tool for linking business partners in a virtual supply chain to reduce resupply times and costs. While the B2C industry receives more attention, the B2B market is significantly larger and rising at a faster rate. B2B organisations are working on new ways to engage their consumers across numerous channels both online and offline in addition to investing in new technologies. Transparent pricing, easily accessible product descriptions, purchase monitoring, and personalised recommendations are among the top e-commerce priorities for many B2B buyers.[280]

EDI which enables the delivery of data straightforwardly, could be referred to as the forefather of B2B e-commerce. Furthermore, researchers have discovered that having a working knowledge of other IT programs made EDI integration easier. As a result, deploying EDI encouraged the adoption of IT such as the Internet and e-CRM, and accelerates the growth of B2B e-commerce.[281] Approximately 80% of online B2B e-commerce is still based on proprietary EDI technologies. Standard transactions such as invoices, bills of lading, shipment schedules, and purchase orders can be sent between two firms via EDI. Even though EDI is still widely used for document automation, it is also used as a method for continuous replenishment by companies that specialise in just-in-time inventory management, which necessitates close coordination with suppliers to ensure that raw materials arrive as production is scheduled to start but no earlier.[282]

---

[279] R. J. Mockler, D. G. Dologit & M. E. Gartenfeld 'B2B E-Business' in S. A. Becker (ed), *Electronic Commerce: Concepts, Methodologies, Tools, and Applications*, Hershey, Information Science Reference, 2008, 9.

[280] Stair & Reynolds, *Principles of Information Systems*, 298.

[281] B. Hernández, J. Jiménez & M.J. Martín, 'Analysis of the Relationship Existing between Business Commercial Information Technologies' in I. Lee (ed), *Transforming E-Business Practices and Applications: Emerging Technologies and Concepts*, Hershey, Information Science Reference, 2010, 262.

[282] Laudon & Laudon, *Management Information Systems*, 401.

The majority of B2B e-commerce activities fall into two categories: those that facilitate the procurement of products and services, and those that support business infrastructure. Single acts of procurement by one organisation from another, as well as organised online trading exchanges, fall into this first type of B2B e-commerce. An individual corporation may run the exchanges as a way to make communication with all of its suppliers easier. In the supply chain or value chain, the other category the B2B business infrastructure covers several business contacts that are not immediately tied to the typical buying and selling of goods and services. The digital business infrastructure for New Economy enterprises is created by the value-added services delivered through these digital networks. Organisations focus on more narrowly defined core skills in this highly networked world, and many procedures are outsourced to firms specialising in providing these real-time digital services.[283]

The use of social media in a B2B environment provides new opportunities to improve the efficiency of the sales force, given the recent rise in the popularity of social media as a new source of data. The internet, specifically social media, is increasingly influencing the B2B sales process. While *Michaelidou et al.* claimed that B2B organisations are slower to adopt social media than B2C companies, the value of social media in a B2B environment has previously been recognised by various academics. *Rodriguez et al*., on the other hand, identified a three-step approach for leveraging social media: creating opportunities, understanding customers, and managing relationships. More publications support the assumption that social media is crucial in B2B selling. Social media is considered an extension of traditional *customer relationship management* (CRM), leading to *social CRM* activities.[284]

B2B and B2C transactions differ from each other in several other ways. To begin with, B2B transactions typically entail large volume orders that can fluctuate from transaction to transaction. In B2B transactions, bulk purchases increase the formality of contracts. Furthermore, B2B transactions can be complicated since they are larger and so include more financial risk. Businesses contending for an order with a new corporate customer may devote a significant amount of time, money, and energy to demonstrate their financial viability so

[283] M. Warkentin (ed), *Business-to-Business Electronic Commerce: Challenges and Solutions*, Hershey, Idea Group Publishing, 2002, vii-viii.
[284] M. Meire et al., 'The added value of social media data in B2B customer acquisition systems: A real-life experiment' *Decision Support Systems*, vol. 104, 2017, 26–37.

that the purchasing company will place an order with them. The seller must ensure that what is delivered meets contractual obligations during the fulfilment process. Finally, business activities between enterprises are carried out across multiple departments, necessitating intra-organisational or inter-organisational coordination and cooperation. Some companies may have a separate procurement department that handles B2B e-commerce.[285]

According to research, B2C companies were quick to embrace social media as a strategic tool, whereas B2B companies struggle to identify and incorporate platforms into their digital marketing mix. Even though social media helps businesses to increase the number of potential relationships, channel management remains narrowly focused on strategic network creation rather than many-to-many communications. As a result, B2B research frequently focuses on how social media is used in specific areas such as sales, key account management, or employer-employee interactions, rather than a more comprehensive examination of its position in the overall channel marketing mix.[286]

An e-commerce company is an entity that partially or exclusively sells products through an online channel. At the business level, the online trading process consists of pre-trade, trade and post-trade activities.[287] Moreover, B2B organisations often have a big profit margin per customer, allowing them to invest in customising the experience for each client. These business technologies are typically utilised to satisfy client needs, improve service, and boost revenue. As a result, the B2B sector is classified into three types of companies. The first group of companies is small businesses. Small firms, by far the most prevalent, are highly fragmented, with a wide range of size, management, and function. Because of this diversity, micro-segmentation is critical, and the approach to a service-based small business will differ significantly from the approach to a product-based small business. A key impediment to reaching this demographic is the difficulty in recognising small businesses. They buy like consumers but do not necessarily act like customers as their aims and motives for buying differ. The next group consists of large organisations, which, unlike small businesses, are easily identifiable and behave similarly. Most large firms have lengthier purchase cycles -

[285] Jelassi & Lopez, *Strategies for e-Business*, 157-158.
[286] S. Iankova et al., 'A comparison of social media marketing between B2B, B2C and mixed business models' *Industrial Marketing Management*, vol.81, 2019, 169-179.
[287] F. M. Aulkemeier et al., 'A pluggable service platform architecture for e-commerce' *Information Systems and e-Business Management*, 2015, 9.

months rather than weeks as well as the purchasing power to buy in bulk. In the case of businesses, the business cycle is also subject to a lot of institutional and regulatory regulation, such as the request for proposal process that is required for purchases. Due to their size and scale, these organisations have significantly more influence over the selling process and negotiating power over market terms than smaller enterprises. This reduces the effectiveness of incentives and rewards in boosting sales. The last group of organisations in the classification is channel marketers. Firms that operate through distributor networks include financial service providers such as insurance companies, technological organisations such as Cisco, manufacturers such as Hewlett-Packard, and general service providers such as ADP. Since distributor networks are individually owned or run, channel marketers are performance-driven and usually employ incentives, recognition, and communications to create a favourable sales environment. Even though the companies are large, the distributor networks operate like small businesses, with commissions and other performance-based payments being typical motivators.[288]

There are two types of B2B e-commerce markets. One is related to the management of material flows in production-oriented supply-chain networks. The other is related to the procurement of *maintenance, repair, and operation* (MRO) items, sometimes referred to as indirect items. Purchases of direct items required in the production of an organisation's products typically are planned well in advance and their procurement is under tight control. On the other hand, while the value of MRO items, or indirect items, is generally much smaller than that of direct items, the cost to process each order is roughly the same. Furthermore, indirect item procurement is easier to modify than production-related procedures, which have already seen significant improvements due to reengineering initiatives over the last decade. Selecting products and vendors, filling out requisition forms, obtaining permissions, sending out purchase orders, receiving the goods, inspecting the content, matching the invoices, and sending out payment are all part of the indirect procurement process.[289]

In B2B systems, e-procurement is the most important area of development. It makes use of the Internet and agent technologies to carry out procurement-related tasks such as buying and selling goods and services, and it will eventually restructure how a company

[288] B. Pearson, *The Loyalty Leap for B2B: Turning Customer Information into Customer Intimacy,* USA, Penguin Special, 2012, 10-11.
[289] M. Shaw et al(eds), *Handbook on Electronic Commerce*, Heidelberg, Springer, 2000, 12.

purchases its items. Negotiating agents play a significant part in e-procurement transactions between two or more businesses. As a result, intelligent agents should be able to negotiate, which will necessitate an understanding of the underlying business logic. Aside from raw data and abstracted information, an agent's understanding gives business insight, promoting wise business. The coordination agents and service agents are the fundamental agents in the agent-based method for multi-market e-procurement.[290]

B2B e-marketplaces have two key advantages. The primary benefit is the speed and efficiency with which information technology allows transactions to be completed. Suppliers and buyers can lower transaction costs by utilising innovative technology. Another advantage is the growing number of participants. E-marketplaces expand options by bringing together a huge number of buyers and vendors. Buyers have a better possibility of obtaining cheaper prices or better transaction circumstances in e-marketplaces since it is easier to find suppliers. When it comes to selling their products, providers can also discover buyers who better match their needs. When the value of a product is determined by the number of users, the product is said to have network effects. Positive network effects are the advantages of having a large number of participants. When a buyer searches for more suppliers, the marketplace's value improves. When there are more suppliers, however, the value of the marketplace reduces for each source. The negative network effects are what they're termed.[291]

Buy-side, sell-side, third-party exchanges and vertical/horizontal marketplaces are the four types of e-marketplaces. Organisations that use e-commerce facilities to procure products or services required by their organisations through immediate buying methods and procurement are known as buy-side e-marketplace applications. There is one buyer and several sellers on the buy side. A sell-side e-marketplace is a website that allows businesses to sell their goods and services to other businesses using a transaction process typically found in an e-business application. On the sell side, there is a single seller and a large number of buyers. A third-party e-marketplace is a neutral e-marketplace that is operated by a third party. It can take the form of a group of companies or a single company that operates the e-marketplace's computer server as well as the e-marketplace's service infrastructure. A

[290] K. A. Nagaty, 'E-Commerce Business Models: Part 2', in I. Lee (ed) *Encyclopaedia of E-Business Development and Management in the Global Economy*, Hershey, Business Science Reference, 2010, vol. I, 365.
[291] B. Yoo, V. Choudhary & T. Mukhopadhyay, 'A model of neutral B2B intermediaries' *Journal of MIS*, vol.19(3), 2003, 43-68.

vertical e-marketplace adds value by handling buyer-seller transactions in a specific industry area. It provides all of the required inputs and strategies to function in the industry. This form of e-marketplace is commonly found to focus solely on a single sector and particular goods and services, such as the chemical industry, construction industry, automobile industry, and so on.[292]

Different viewpoints may be used to distinguish e-marketplaces. At the heart of every transaction, the function is the market mechanism. Two differentiators are defined from this perspective: pricing mechanism and market access. Access to the market may also be used to classify e-marketplaces. E-marketplaces can be divided into two types: open and closed e-marketplaces. The categorisation of e-marketplaces based on the types of parties involved in transactions is perhaps one of the most common classifications. Any transaction is likely to involve three different types of parties: the business, the client - the recipient of the finished good or service, and the government. The structure and horizon of the relationship between businesses and e-marketplaces is another criterion used to distinguish various types of e-marketplaces. An e-marketplace can be interpreted as a long-term systemic sourcing solution or a short-term spot-sourcing solution from this perspective. Another way to distinguish e-marketplaces is to look at how products/services are applied in vertical/horizontal e-marketplaces. From this point of view, e-marketplaces can be divided into two groups: a) those that provide direct goods, and b) those that provide indirect goods. E-marketplaces may be classified as hierarchical (biased) or market-driven based (third party) on the e-marketplace bias. E-marketplaces can be classified into three groups from the standpoint of stakeholders: a) buyer-oriented, b) seller-oriented, and c) neutral e-marketplaces. E-marketplaces can be divided into three categories based on who owns them: a) buyer-side or seller-side, where a major market player - the buyer/seller - owns and operates the e-marketplace; b) neutral or third party, where an impartial third party sets up and operates the e-marketplace; and c) consortia, where many major market players, like buyers, sellers, and/or intermediaries come together to set up and operate the e-marketplace.[293]

---

[292] N. Jailani 'Concept of an Agent-Based Electronic Marketplace' in I. Lee (ed) *Encyclopaedia of E-Business Development and Management in the Global Economy*, Hershey, Business Science Reference, 2010, 241-242.
[293] K. M. Lavassani, B. Movahedi & V. Kumar, 'From Integration to Social Media: Understanding Electronic Marketplace' in Lee (ed) *Trends in E-business, E-services, and E-Commerce: Impact of Technology on Goods, Services, and Business Transactions*, Hershey, Business Science Reference, 2014, 6-12.

A corporation must follow very meticulous procedures in order to get ready for a successful entry into an e-marketplace. Only by employing this strategy will the company be able to take full advantage of the chances at hand and produce the desired business results. Investigating the elements that businesses must take into account for a successful e-marketplace implementation is crucial. If organisations are aware of these aspects, they will be better equipped to implement the e-marketplace successfully and, as a result, will be able to compete in the global market. Organisational, e-marketplace, and environmental aspects are the three groupings of elements that organisations should take into account when making e-marketplace decisions, according to previously published study findings and interviews with industry experts.[294]

3.2.1. Regulation of B2B transactions

The legal framework for B2B transactions is also very specific with its guidelines, regulations and reports. One of the main reasons for choosing this legal framework and the case law associated with it is that its interpretation and application allow understanding and gaining insight into the working perception of B2B transactions in general.

3.2.2. Misleading and comparative advertising

Comparative advertising that was deceptive or illegal might distort competition within the internal market. Advertising had an impact on the economic well-being of consumers and traders, regardless of whether it generated a contract. The differences in advertising legislation between the MS mislead businesses obstruct the execution of advertising campaigns across national borders and affected the free movement of products and provision of services. It was necessary to set minimum and objective criteria for determining if advertising was deceptive. However, for comparative advertising to be effective, it might be necessary to identify a competitor's goods or services by referring to a trade mark or trade name that the latter owned. As a result, action at the European level was required, which was

[294] A. Pucihar & M. Podlogar 'E-Marketplace Adoption Success Factors: Challenges and Opportunities for A Small Developing Country' in S. Kamel (ed) *Electronic Business in Developing countries: Opportunities and Challenges*, Hershey, Idea Group Publishing, 2006, 90-91.

accomplished by the adoption of Directive 2006/114/EC on misleading and comparative advertising (MCAD). The adoption of the MCAD was the ideal tool since it established uniform broad principles while allowing MS to choose the best form and manner for achieving these goals. It conformed with the subsidiarity principle. The goal of MCAD was to safeguard traders against misleading advertising and the unfair consequences that could result from it, as well as to establish the conditions under which comparison advertising was permitted. Under the MCAD, 'advertising' was defined as making a representation in any form in connection with a trade, company, craft, or profession to promote the provision of products or services, including immovable property, rights, and responsibilities. 'Misleading advertising' was defined as any advertising that deceived or was likely to deceive the persons to whom it was addressed or reached in any way, including its presentation, and which, as a result of its deceptive nature, was likely to affect their economic behaviour or injures or was likely to injure a competitor. Any advertising that directly or implicitly identified a competitor or the goods or services offered by a competitor was referred to as 'comparative advertising.' Comparative advertising might be an acceptable technique for alerting consumers of their benefit if it compared material, relevant, verifiable, and representative attributes and was not deceptive. It was preferable to establish a comprehensive definition of comparison advertising that included all types of comparative advertising. By the Treaty, the MS should be free to choose the forms and methods for implementing these conditions, unless those forms and methods were already defined by MCAD. In the interests of merchants and competitors, MS must guarantee that adequate and effective mechanisms exist to prevent deceptive advertising and enforce compliance with comparable advertising regulations. Since Directive 84/450/EEC[295] has been repealed, any references to it should be read as references to the MCAD which entered into force on December 12, 2007.[296]

Advertising has a significant economic impact on businesses because it is an important component of any business strategy. It is a key component of commercial success since it helps traders to present their goods and services. It can also boost competition by giving customers more information and allowing them to compare items. Businesses can reach

[295] Council Directive 84/450/EEC, OJ L 250, 19.9.1984, 17–20.
[296] Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising (codified version) (Text with EEA relevance) OJ L 376, 27.12.2006, 21–27.

customers in every corner of the EU with a commercial message due to the Single Market. Small firms, which form the backbone of the European economy, are particularly vulnerable to misleading marketing because they lack the resources to defend themselves and require a clear structure that protects fair competition and provides effective enforcement tools. The EU's rules on B2B advertising are designed to ensure that businesses employ truthful marketing and advertising. While the completely harmonised laws on comparable advertising have been uniformly adopted, there was a wide range of restrictions that go beyond the minimal EU-wide protection against misleading advertising, according to information acquired by the Commission on all MS legal systems. Some MS chose to go beyond the MCAD's minimum legal standard and extend the UCPD's level of protection to B2B relationships, either partially or entirely. As a result, the level of protection provided to European enterprises varies, leaving companies unsure of their rights and responsibilities in cross-border circumstances. The requirements imposed by the MCAD were fairly restricted in terms of enforcement procedures. Currently, MS were enforcing MCAD using a variety of national procedures. The key distinction was whether or not public enforcement was possible. Authorities in some MS had the power to prosecute rogue traders, whereas, in others, only victims could seek recourse. Such discrepancies, particularly in cross-border advertising, had a significant impact on the effective level of protection. The Commission identified the following drivers of problems in the area of cross-border misleading marketing practices in its 2012 Communication: a) lack of effective enforcement, b) unclear and insufficient rules on misleading marketing practices, and c) SMEs' lack of awareness of the illegality of misleading marketing practices.[297]

The MCAD was referenced in the 'Fitness Check' as the legal background for B2B sphere transactions. The MCAD primarily protects traders from deceptive B2B marketing. They apply to both online and offline transactions, as well as domestic and cross-border transactions. It also establishes uniform comparable advertising guidelines that apply to both B2B and B2C advertising. These guidelines are intended to ensure that comparison advertising compares 'like with like,' is objective, does not disparage or degrade other

[297] European Commission, 'Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions Protecting businesses against misleading marketing practices and ensuring effective enforcement', Brussels, 27.11.2012 COM (2012) 702 final.

companies' trademarks, and does not cause traders to become confused. Following the UCPD's carve-out of B2C unfair commercial practices, the present MCAD consolidates the remaining sections on B2B misleading advertising and comparable advertising. The MCAD is a hybrid mechanism. Its provisions against B2B misleading advertising provide a minimal level of harmonisation. On the other hand, its provisions on comparable advertising are fully harmonised, similar to those of the UCPD. The scope of the MCAD is limited to 'advertising' as this was the mechanism used in the original 1984 Council Directive 84/450/EEC against misleading advertising, which incorporated the comparative advertising rules in 1997. Although the concept of 'advertising' in EU law, including the MCAD, is broad, it is narrower than the UCPD's concept of 'commercial practices.' The MCAD forbids generalised misleading advertising. Unlike UCPD, MCAD does not provide examples; instead, it simply outlines the factors to consider when determining whether an advertisement is misleading (Art.3).[298]

The relevance of the Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (UCTD) in B2B relationships was one of the concerns examined in the 'Fitness Check'. According to the Lot 1 Study, several MS already have laws in place to safeguard firms from unfair contract terms, which are generally found in general contract law provisions and complemented by supplementary, often sector-specific rules. The Lot 1 study recommended expanding the UCTD to protect SMEs because of the similarities and minor variations in knowledge, expertise, and negotiating power between small businesses and consumers, which have been highlighted in numerous country research. However, the 'Fitness Check' consultation revealed a wide range of opinions on the extension of the UCTD, with many industry organisations and government agencies opposing the concept. While over half of the respondent businesses (54%) thought the UCTD's scope of application should be extended to B2B contracts, business associations mostly disagreed (24% agree vs. 38% disagree) and public authorities had mixed feelings and did not show much support in the online public consultation (21% agree v. 21% disagree). Under the Lot 1 Study, stakeholders from a large number of MS agreed that the MCAD's principle-based approach provided a fairly strong legal framework for a big portion of the B2B advertising industry. Several stakeholders, on the other hand, stated that they had no knowledge of MCAD and that no

[298] European Commission, 'Report of the Fitness Check, Brussels, SWD (2017) 209 final, 70.

administrative or judicial action was taken, while other stakeholders emphasised that false advertising is damaging to small businesses in particular. Furthermore, there is little practical experience with MCAD enforcement across borders. While differences in the application of the principle-based approach and the minimal harmonisation nature of rules on misleading advertising could harm cross-border trade on a theoretical level, the Lot 1 Study found no substantial issues in this regard. The online public consultation provided several proposals for changing the MCAD, for example, the vast majority of business respondents agreed that a blacklist of B2B operations should be implemented.[299]

In the *Belgian Electronic Sorting Technology* case (C-657/11) the Court sought to ascertain whether Art.2(1) of Directive 84/450 and Art.2(a) of Directive 2006/114 must be interpreted as meaning that the term 'advertising', as defined by those provisions. For that reason, the account must be taken of the purpose of Directives 84/450 and 2006/114, which is, as is apparent from Art.1 in each of those directives, to protect traders against misleading advertising and its unfair consequences and to lay down the conditions under which comparative advertising is permitted. The purpose of those conditions, as the Court held that it is apparent to achieve a balance between the different interests which may be affected by allowing comparative advertising, by allowing competitors to highlight objectively the merits of the various comparable products to stimulate competition to the consumer's advantage while, at the same time, prohibiting practices which may distort competition, be detrimental to competitors and hurt consumer choice. It follows from recitals and definitions that the EU legislature had the intention of establishing, using those directives, a complete framework for every form of advertising event, whether or not it induces a contract, to avoid such advertising harming both consumers and traders and leading to distortion of competition within the internal market. Consequently, the term 'advertising', within the meaning of Directives 84/450 and 2006/114, cannot be interpreted and applied in such a way that steps taken by a trader to promote the sale of his products or services that are capable of influencing the economic behaviour of consumers and, therefore, of affecting the competitors of that trader, are not subject to the rules of fair competition imposed by those directives. In light of the foregoing, the answer to the question referred to is that Art.2(1) of Directive 84/450 and Art.2(a) of Directive 2006/114 must be interpreted as meaning that the term 'advertising', as

[299] European Commission, 'Report of the Fitness Check', SWD (2017) 209 final, 71.

defined by those provisions, covers, in a situation such as that at issue in the main proceedings, the use of a domain name and that of metatags in a website's metadata. In contrast, domain name registration as such is not covered by this term.[300]

Thus, the purpose of MCAD is to protect traders from misleading advertising from other B2B companies, which amounts to unfair business practices. To this goal, MCAD establishes the terms that authorise comparison advertising. Advertisements that deceive or have the potential to deceive the recipients are prohibited. These commercials' misleading character may have an impact on consumer and trader economic behaviour, or it may hurt a rival. Comparative advertising makes mention of a competitor or competing products or services, either directly or indirectly. Only when the advertising is not misleading it is acceptable and it may be a proper way to inform customers of what is in their best interests.

3.2.3. Fairness and transparency for business users of online intermediation services

The employment of online intermediation services has been enthusiastically received by consumers. Increasing transparency and trust in the internet platform economy in B2B relationships may indirectly aid to increase consumer trust in the online platform economy. The nature of the connection between providers of online intermediation services and business users may result in instances where business users have limited options for seeking redress when providers of those services take unilateral measures that result in a dispute. To provide a fair, predictable, sustainable, and trusted online business environment within the internal market, the EU legislators adopted Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services or so-called Platform-to-Business Regulation (P2B Regulation).[301] Business users of online intermediation services should be afforded appropriate transparency and effective redress options across the EU to facilitate cross-border business within the Union, improve the proper functioning of the internal market, and address possible emerging fragmentation in the specific areas covered by this Regulation. Since online intermediation services and online search engines are often

[300] *Belgian Electronic Sorting Technology*, C-657/11, Judgment of the Court (Third Chamber), 11 July 2013, para. 39-60.
[301] Platform-to-business trading practices <https://digital-strategy.ec.europa.eu/en/policies/platform-business-trading-practices> accessed 08 Aug. 2023.

global, this Regulation should apply to suppliers of those services whether they are based in the MS or outside the Union, as long as two cumulative conditions are met. To begin, business users or corporate website users must be registered in the EU. Moreover, business users or corporate website users should, at least for part of the transaction, offer their goods or services to consumers in the EU through the provision of those services. Online e-commerce marketplaces, including collaborative ones with business users, online software application services, such as application stores, and online social media services, regardless of the technology used to provide such services, are examples of online intermediation services covered by this Regulation. The definition of 'an online search engine' used in this Regulation should be 'technology-neutral', given the rapid pace of innovation. The purpose of P2B Regulation is to promote the proper functioning of the internal market by establishing rules that ensure appropriate transparency, fairness, and effective redress options received by business users of online intermediation services and corporate website users about online search engines. This Regulation applies to online intermediation services and online search engines that are provided or offered to be provided, to business users and corporate website users who have their place of establishment or residence in the Union and who, through those online intermediation services or online search engines, offer goods or services to consumers in the Union, regardless of the providers' place of establishment or residence. P2B Regulation does not apply to online payment services, online advertising tools, or online advertising exchanges that are not supplied to enable direct transactions and do not include a contractual connection with consumers. This Regulation applies without prejudice to EU law in the fields of judicial cooperation in civil matters, competition, data protection, protection of trade secrets, consumer protection, e-commerce and financial services.[302]

According to P2B Regulation, a 'business user' is defined as a private individual acting in a commercial or professional capacity, or a legal entity that, through online intermediation services, offers goods or services to consumers for purposes related to its trade, business, craft, or profession. 'Online intermediation services' are defined as services that meet all of the following criteria: a) they are information society services as defined in point (b) of Art.1(1) of Directive (EU) 2015/1535; b) they enable business users to make goods or services

[302] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (Text with EEA relevance) PE/56/2019/REV/1 OJ L 186, 11.7.2019, 57–79.

available to consumers to facilitate the start of direct transactions between those business users and consumers, regardless of where such transactions are eventually completed; c) they are given to business users under contractual agreements between the service provider and business users that sell goods or services to consumers. The term 'online search engine' refers to a digital service that allows users to enter queries to perform searches of all websites, or all websites in a specific language, based on a query on any subject in the form of a keyword, voice request, phrase, or other input, and returns results in any format in which information related to the requested content can be found. 'Provider of online intermediation services' refers to any natural or legal person who provides, or offers to provide, online intermediation services to business users, whereas 'provider of online search engine' refers to anyone who provides, or promises to provide, online search engines to consumers.[303]

There are 'Guidelines' to make it easier for providers of online intermediation services and providers of online search engines to comply with and enforce the standards set out in Art.5 of Regulation (EU) 2019/1150. These Guidelines are also intended to assist providers in applying the requirements and to help streamline how key ranking elements are identified and presented to business customers and users of corporate websites following Art.5(7) and Rec.28 of the Regulations. Simultaneously, this Regulation aims to achieve this goal by not requiring providers to disclose algorithms or any other information that could reasonably rely upon, could deceive consumers or cause harm by manipulating search results (Art.5(6)). As a result, providers are not forced to divulge the details of how their ranking methods, including algorithms, work, and their capacity to respond to bad faith ranking manipulation should not be harmed (Rec.27).

Given the partially divergent legal requirements for providers of online intermediation services and providers of online search engines, as outlined in Art.5, and the distinct nature of the services in question, the content of the required description of the main ranking parameters will inevitably differ between these two types of services. Furthermore, as noted in Rec.25, the substance of online intermediation services, particularly the quantity and kind of primary criteria, might differ significantly between providers. The guidance in these Guidelines should not be followed blindly, but rather with care, taking into account all of the relevant facts and circumstances in each case. These guidelines are without prejudice to the

[303] Ibid, Art.2.

providers' responsibilities for ensuring compliance with the requirements of Art.5, as well as the powers and responsibilities of the MS' competent authorities and courts for enforcing those requirements following the Regulation and other EU laws. The interpretation of the requirements is ultimately up to the CJEU.[304]

The Observatory on the Online Platform Economy, using a review of the terms and conditions (T&Cs) of a sample of platforms, conducted preliminary monitoring of the EU P2B Regulation's implementation between late 2020 and early 2021. Three categories of platforms were discovered as a result of this monitoring: a) platforms that appear to fall under the purview of the P2B Regulation and whose T&Cs appear to have been modified in reaction to its implementation, or provide information on its requirements; b) platforms that appear to fall under the purview of the P2B Regulation, whose publicly available T&Cs do not appear to have been modified, and which lack openness about several issues addressed by the P2B Regulation and c) platforms whose T&Cs do not appear to have been updated or modified in response to the Regulation's application and may or may not fall under the purview of the P2B Regulation. The majority of the businesses who participated in the business user survey reported having experiences that seemed to be compliant with the Regulation, and they had not noticed any substantial changes in the transparency offered by the platforms they use. There was no information yet on how well the internal complaint-handling procedures worked. Online forums for business users have received some information about P2B Regulation implementation problems, including information about arbitrary account limits, listing suspensions, and the absence of efficient complaint processing procedures.[305]

So, by providing business users of online platforms with more effective options for redress when they encounter problems and by establishing a predictable and innovation-friendly regulatory environment for online platforms within the EU, P2B Regulation aims to ensure that business users are treated fairly and transparently by these platforms. To link EU businesses and professional websites with EU consumers, the regulation creates new rules for online intermediary services, including online platforms and online search engines. Online platform providers must designate one or more mediators that business users can contact to

[304] Commission Notice, 'Guidelines on ranking transparency pursuant to Regulation (EU) 2019/1150 of the European Parliament and of the Council (2020/C 424/01)' C/2020/8579, OJ C 424, 8.12.2020, 1–26.
[305] European Commission, 'Directorate-General for Communications Networks, Content and Technology, Study on Support to the observatory for the online platform economy': Final report', Publications Office, 2021, 9.

resolve any disagreements with the appropriate online platform provider to further facilitate rapid and efficient dispute resolution.

3.2.4. Late payment in commercial transactions

Many payments in commercial transactions between economic operators and public agencies are made after the contract or the broad commercial conditions have been agreed upon. Even though the items are delivered or services are rendered, many of the associated invoices are paid much after the deadline. Late payments hurt liquidity and make financial management more difficult for businesses. When a creditor needs to get external finance due to late payment, it has an impact on their competitiveness and profitability. During moments of economic crisis, when access to funding is more difficult, the danger of such unfavourable consequences grows dramatically. Lawsuits relating to late payment were already facilitated by Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, Regulation (EC) No 805/2004 on establishing a European Enforcement Order for undisputed claims, Regulation (EC) No 1896/2006 establishing a European payment procedure and Regulation (EC) No 861/2007 establishing a European small claims procedure. However, to deter late payment in business transactions, further requirements must be established. Since, for reasons of clarity and rationality, significant changes to Directive 2000/35/EC[306] and new reformulation of the relevant sections were required, the EU legislators subsequently adopted a new Directive 2011/7/EU on combatting late payment in commercial transactions. This Directive's scope should be restricted to payments made as remuneration for commercial transactions. This Directive should not apply to consumer transactions, interest on other payments, such as payments made under the laws governing checks and bills of exchange, or payments made as compensation for damages, such as payments made by insurance firms. Given that public authorities manage a significant volume of payments to companies, this Directive should regulate all commercial transactions, whether they were conducted between private or public undertakings, or between undertakings and public authorities. 'Late

[306] Directive 2000/35/EC of the European Parliament and of the Council of 29 June 2000 on combating late payment in commercial transactions, OJ L 200, 8.8.2000, 35–38.

payment' is a contract breach that is made financially appealing to debtors in most MS by low or no interest rates assessed on late payments or lengthy redress procedures. To reverse this pattern and discourage late payment, a significant transition to a culture of prompt payment was required, especially one in which the absence of the right to charge interest should always be regarded as a fundamentally unfair contractual term or practice. This change should also include the addition of specific provisions on payment terms and creditor compensation for costs incurred, as well as the presumption that the exclusion of the right to compensation for recovery costs was highly unfair. As a result, it was recommended that B2B contractual payment terms be limited to 60 calendar days as a general rule. However, when undertakings require longer payment periods, the parties should be permitted to expressly agree on payment terms that are longer than 60 calendar days, as long as the extension is not unduly unfair to the creditor. To avoid jeopardising the attainment of this Directive's goal, MS should ensure that the maximum duration of an acceptance or verification procedure in commercial transactions did not exceed, in general, 30 calendar days. However, in some cases, such as in the case of especially complex contracts, a verification procedure might be extended beyond 30 calendar days if specifically stipulated in the contract and associated tender documents, and provided if it was not unreasonably unfair to the creditor. In cases where late payment interest is due in commercial transactions under Articles 3 or 4, MS must ensure that the creditor is entitled to at least receive a set sum of 40€ from the debtor. Since the goal of this Directive, namely combating late payment in the internal market, could not be adequately achieved by MS and, as a result, could be better achieved at the EU level due to its scale and effect, the Union might take measures by the principle of subsidiarity as set out in Art.5 of the TEU. Directive 2000/35/EC has been superseded by this Directive, which entered into force on 16 March 2013, but contracts concluded before that date, to which this Directive did not apply by Art.12(4), should still be governed by it.[307]

As part of the REFIT review, Directive 2011/7/EU was examined in terms of the achievement of its objectives and proposals for improving its implementation. A clear ex-post review was challenging due to three key factors: a) the Directive's recent implementation, b) the difficulty of determining how the Directive affected developments on the ground, and c)

[307] Directive 2011/7/EU of the European Parliament and of the Council of 16 February 2011 on combating late payment in commercial transactions Text with EEA relevance OJ L 48, 23.2.2011, 1–10.

exogenous factors like the financial crisis and the economic standing of some MS. As the Directive was still in its early stages of development at the time, there were few improvements in typical payment periods. Although businesses have been well aware of their rights under this Directive, they have not yet been widely disseminated. This Directive, on the other hand, was judged to be in line with other EU legislation and policies, was still relevant, and adds value to the EU.[308]

By making late payment less appealing for debtors or compensating creditors for late payment practises, Directive 2011/7/EU on Late Payment sought to modernise and reinforce Directive 2000/35/EC. Payment deadlines, statutory interests, flat-rate compensation, enforceable title, the favourability principle for the creditor, and, finally, provisions against unfair payment practise and clauses were the five key components that Directive 2011/7/EU focused on. The regulatory framework created by the implementation of Directive 2011/7/EU has made EU MS more aware of the problems with late payments. A country-specific investigation showed that the construction industry continues to see a lot of commercial connections with late payments. Two main conclusions may be drawn from the study as a result: 1) there is a need for more regular and consistent data, and 2) there is a need for greater coordination among programmes and between public and private sector actors. To combat the problem of late payments, the EC also employs indirect rules like the EU Directive on Public Procurement. Another effective strategy to deal with late payments appears to be closer monitoring and reporting of payment behaviour in the construction sector, along with potential sanctions.[309]

In the *RL case* (C-199/19), the Court tried to find an answer to the question, of whether Art.2(1) of Directive 2011/7 must be interpreted as meaning that a contract under which the main obligation is the provision, for payment, of property for temporary use, such as a lease or rental agreement for business premises, is a commercial transaction for that provision and therefore falls within the material scope of that directive. Art.2(1) of Directive 2011/7 sets out two conditions that must be satisfied for a transaction to fall within the concept of

[308] European Commission, 'Report from The Commission to The European Parliament and The Council on the implementation of Directive 2011/7/EU of the European Parliament and of the Council of 16 February 2011 on combating late payment in commercial transactions' {SWD (2016) 278 final} 9.
[309] European Construction Sector Observatory, 'Late payment in the construction sector', Analytical Report, 2020, 8-9.

'commercial transactions' within the meaning of that provision. It must, initially, be carried out either between undertakings or between undertakings and public authorities and, furthermore, lead to the delivery of goods or the provision of services for remuneration. As regards the first condition, it should be recalled that the concept of 'undertaking' is defined in Art.2(3) of Directive 2011/7 as 'any organisation, other than a public authority, acting in the course of its independent economic or professional activity, even where that activity is carried out by a single person'. In the main proceedings, it is common ground that *RL*, which is a limited liability company, has the status of 'undertaking' within the meaning of Art.2(3) of that directive. On the other hand, Directive 2011/7 provides no list of the various types of contracts which entail the delivery of goods or a provision of services as referred to in Art.2(1) thereof. Secondly, lease or rental agreements are not included among the transactions and payments made in fields that, according to Rec.8 of Directive 2011/7, fall outside the scope of that directive. In light of all the foregoing considerations, the answer to the first question is that Art.2(1) of Directive 2011/7 must be interpreted as meaning that a contract under which the main obligation is the provision, for payment, of property for temporary use, such as a lease or rental agreement for business premises, is a commercial transaction leading to a provision of services, within the meaning of that provision, provided that that transaction is between undertakings or between undertakings and public authorities.[310]

Therefore, by requiring prompt payment of bills, Directive 2011/7/EU seeks to protect businesses, especially SMEs from late payments in commercial transactions. Additionally, Directive 2011/7/EU establishes deadlines for paying invoices and offers financial penalties if these are not followed. Unless otherwise specifically stipulated in the contract and given that the provisions are not blatantly unjust to the creditor, businesses must pay invoices within a maximum of 60 days. Within 30 days, public entities must make payment for the products and services they purchase. The timeframe may be extended in extraordinary cases, such as the healthcare industry or for particular industrial or commercial activity, to 60 days. Creditors who have met their contractual and legal duties but have not received payment within the allotted time frames are entitled to interest (8%) and other penalties for the late payment. Debtors must pay creditors a minimum fixed amount of 40€. They also have a right to

[310] *RL* (C-199/19) Judgment of the Court (Ninth Chamber) of 9 July 2020, paras 21-41.

reimbursement for any further reasonable efforts required to recover the debt, such as legal fees or hiring a debt collection agency.

3.2.5. Summary

B2B e-commerce transactions, being much larger and growing at a faster pace, lead to partnerships between two or more businesses. In B2B e-supply chain management, it is good to achieve maximum sales growth at the lowest possible cost by optimising the supply chain. On the other hand, e-procurement is a method of integrating supply-side activities to better control overall purchasing costs and ensure supply chain integration. When managing and controlling a B2B transaction, entrepreneurs must remember to avoid misleading and comparative advertising for the sake of better transactions and profitable transaction results. Another factor of B2B transactions is that for business users of online intermediation services, there is a demand for fairness and transparency as they provide a fair, predictable, stable and reliable online business environment in the domestic market. Regarding late payment, it is worth setting a general rule of 60 calendar days for payment under a B2B contract to reduce administrative burden and encourage entrepreneurship. Thus, when businesses want to construct a B2B e-commerce environment in the future, they should consider the aforementioned legal frameworks as a ‘legislative compass’ in the domestic market.

3.3. The concept of the vulnerable individuals in the EU consumer protection law

Consumer protection laws are intended to assist final consumers in their market transactions by preventing or fixing market imperfections. Consumer law can address the health and safety implications of market transactions as well as information inefficiencies like incomplete information, information asymmetries, or even restricted rationality. Making free and informed judgements is achievable when consumers have access to information that is

both high quality and affordable.[311] The regulation of social components of the market, such as consumer safety and health, is another focus of consumer protection law.[312]

Several major legal provisions in the EU deal with consumer protection. Art.4 of the TFEU refers to the field of consumer protection as one of the main areas of shared competence between the Union and the MS. According to Art.169 of the TFEU, to promote consumer interests and ensure a high level of consumer protection, the Union should contribute to protecting consumers' health, safety, and economic interests, as well as promoting their right to information, education, and to organize themselves to safeguard their interests.[313] The Art.38 of the EU Charter also mentions that the Union policies should ensure a high level of consumer protection.[314] There are also specific directives and regulations on the EU secondary legislation that deals with matters of consumer protection.

Since it was important to remove unfair provisions and protect consumers when purchasing goods and services under contracts governed by the laws of the MS other than their own, Directive 93/13/EEC on unfair terms in consumer contracts (UCTD) was adopted by the EU legislators on 5 April 1993. The goal of this Directive was to harmonise the MS' laws, regulations, and administrative rules regarding unfair terms in contracts between a seller or supplier and a consumer. Contractual terms that reflected mandatory statutory or regulatory provisions, as well as laws or principles of international conventions to which the MS or the Community were parties, were exempt from the provisions of UCTD, particularly in the transport sector. According to UCTD 'consumer' means any natural person who, in contracts covered by this Directive, is acting for purposes which are outside his trade, business or profession, while 'seller or supplier' means any natural or legal person who, in contracts covered by this Directive, is acting for purposes relating to his trade, business or profession, whether publicly owned or privately owned. The 'unfair terms' was defined in Art.3, as a contractual term which has not been individually negotiated and should be regarded as unfair if, contrary to the requirement of good faith, it caused a significant imbalance in the parties'

---

311 Kati J. Cseres, 'The Controversies of the Consumer Welfare Standard' *The Competition Law Review*, vol.3/2, 121-173.

312 Inge Graef 'Blurring Boundaries of Consumer Welfare: How to Create Synergies Between Competition Consumer and Data Protection Law in Digital Markets' in Mor Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law, MPI Studies on Intellectual Property and Competition Law 28*, Germany, Springer-Verlag GmbH, 2018, 126.

313 TFEU, Art.169.

314 Charter of Fundamental Rights, Art.38.

rights and obligations arising under the contract, to the detriment of the consumer. Contracts should be written in plain, understandable language, the consumer should be allowed to evaluate all terms, and if in question, the consumer's preferred interpretation should prevail. However, because UCTD also applied to trades, businesses, or professions of a public nature, MS must ensure that unfair terms were not included.[315] Therefore, the UCTD protects EU consumers from unfair terms and conditions that could be found in a standard contract for goods and services that they buy. To avoid any significant disparity in the parties' rights and obligations, the UCTD references the concept of 'good faith' and includes a non-exhaustive list of unfair contract terms. When it comes to the use of the term, it should be interpreted in a way that is beneficial to the consumer. Consumers do not commit to contract terms that are considered unfair, but the remainder of the contract is still enforceable if permitted by law.

The CRD 2011/83/EU, which replaced the two previous directives - the doorstep selling Directive (85/577/EEC) and the distance selling Directive (97/7/EC), sought to improve consumer protection by harmonising several important facets of national laws governing contracts between consumers and businesses and by promoting trade between MS, particularly for those making online purchases. As a result, CRD should establish standard rules for the common aspects of distance and off-premises contracts, departing from the previous Directives' minimum harmonisation approach while enabling MS to preserve or adopt national regulations in particular areas. Compared to the tremendous growth of domestic distance selling, the discrepancy in the cross-border distance selling particularly in the services sector was noticeable in e-commerce, which had plenty of room for expansion. Therefore, full harmonisation of consumer information and the right of withdrawal in distance and off-premises contracts would lead to increased consumer protection and improved internal market functioning. The CRD delivered requirements for providing information for distance contracts, off-premises contracts, and contracts that were not distance or off-premises contracts. The CRD also governed the right of withdrawal for distance and off-premises transactions, as well as harmonised certain regulations concerning performance and other aspects of B2C contracts.[316] The CRD was later amended by Directive (EU) 2019/2161 of 27

[315] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts OJ L 95, 21.4.1993, 29–34.
[316] Directive 2011/83/EU, OJ L 304, 64–88.

November 2019, on the better enforcement and modernisation of Union consumer protection rules, thus broadening the scope of the CRD.[317]

The internal market's full potential can only be realised if all market participants have easy access to cross-border sales of goods, especially through e-commerce transactions. An increasing market for goods that contain or are interconnected with digital content or digital services has resulted from technological advancements. Because of the expanding number of such devices on the market and their rapid adoption by consumers, action at the EU level is required to ensure a high level of consumer protection and legal certainty about the rules that apply to contracts for the sale of such products. MS has been given the freedom to go above and beyond the Union's requirements, introducing or maintaining legislation that assured an even better level of consumer protection. Since certain aspects of contracts for the sale of goods should be harmonised based on a high level of consumer protection to achieve a Digital Single Market, increase legal certainty and reduce transaction costs, the EU legislators enacted the Directive (EU) 2019/771 on certain aspects concerning contracts for the sale of goods on 20 May 2019. The purpose of this Directive is to contribute to the proper functioning of the internal market while ensuring a high level of consumer protection by establishing common rules on certain requirements relating to sales contracts concluded between sellers and consumers, in particular rules on goods conformity with the contract, remedies in the event of a lack of such conformity, the modalities for exercising those remedies, and commercial guarantees. This Directive is applied to sales contracts between a consumer and a seller. Under this Directive, contracts between a consumer and a seller for the provision of items to be manufactured or produced are also considered sales contracts. This Directive does not apply to any tangible medium which serves solely as a medium for digital content, or any goods sold by way of execution or otherwise by operation of law. This Directive complemented Directive 2011/83/EU. While Directive 2011/83/EU primarily addressed pre-contractual information requirements, the right of withdrawal from a distance and off-premises contracts, and rules on delivery and risk transfer, this Directive added rules on goods conformity, remedies in the event of non-conformity, and modalities for exercising those remedies.[318]

[317] Directive (EU) 2019/2161, OJ L 328, 7–28.
[318] Directive (EU) 2019/771, OJ L 136, 28-50.

Uncertainty about important contractual rights and the lack of a clear contractual framework for digital material or digital services were two major problems contributing to consumers' lack of confidence. That's why Directive (EU)2019/770 was adopted by the EU legislators to contribute to the proper functioning of the internal market while ensuring a high level of consumer protection by establishing common rules. The new rules apply to a) whether digital content or a digital service conforms with the contract; b) the methods for exercising remedies in the event of a failure to comply with the contract or a lack of supply; and c) the digital content or a digital service's modification. This Directive lays down general rules about certain requirements relating to contracts between traders and consumers for the supply of digital content or a digital service. This Directive addresses issues related to the various categories of digital content, digital services and their supply. The scope of this Directive extends to any contract where the trader supplies or undertakes to supply digital content or digital service to a consumer and the consumer pays or undertakes to pay a price. This Directive and Directive (EU) 2019/771 should complement each other. While this Directive establishes rules for certain requirements relating to contracts for the supply of digital content or services, Directive (EU)2019/771 establishes rules for certain requirements relating to contracts for the sale of goods. Furthermore, the requirements of Directive 2011/83/EU should continue to apply to such tangible media and the digital material provided on it, including the right of withdrawal and the nature of the contract under which those products are supplied. This Directive is also unrelated to the copyrighted distribution rights that apply to these products and the requirements for the lawful processing of personal data, which are subject to Regulation (EU) 2016/679.[319]

3.3.1. The concept of the average consumer in the EU consumer protection law

The consumer notion plays a crucial role in setting a benchmark, making it particularly significant in EU law. This is evident in a variety of situations, the two most important of which are probably determining whether national provisions are appropriate and determining whether commercial communications violate required standards (for example, whether they should be found to be aggressive or misleading for purposes of unfair commercial practices

[319] Directive (EU) 2019/770, OJ L 136, 1–27.

law). The chosen image conveys a lot about what can be expected of both businesses and consumers, which clarifies the nature and character of EU consumer law.[320]

The theoretical presumption of who/what is the average consumer and simple terminology are part of the problem before getting to its substantive meaning and effects. The legal context of various other 'consumer' versions that co-exist across the domains of overarching EU law must be taken into consideration when analysing the average consumer in European law. These variations each have unique traits, but they all serve as a sort of legal lookalike of the European 'consumer' for the legislative and judicial branches of government in a particular area of EU law. As a result, even though the evidence is tainted with a high degree of normativity and uncertainty, the average consumer is not seen as bipolar, either because it is legal fiction or because it is descriptive. Additionally, courts ultimately define the average consumer in law. The CJEU's case law also shows that the typical consumer is not purely descriptive.[321]

Both the national legislation and the EU law use the 'average consumer' as a normative benchmark. It is crucial to understand how the standard is applied by courts and how its normative content is shaped to fully comprehend its value as an analytical tool in post-national law-making. It is possible to distinguish between two features, the first of which has to do with how the standard works and the second with how courts determine its normative setting. In contrast, when asked to interpret EU consumer law Directives, the CJEU typically adopts a very pro-consumer attitude. In other words, while the Court actively opposes national legislation that can obstruct commerce, positive harmonisation of national (private) laws through Directives is aided by the Court's expansive and consumer-friendly interpretation of those laws. These demonstrate that the CJEU, not only in its free movement case law but also in its interpretation of Directives, views the idea as a conciliation mechanism between EU law and national laws. Numerous EU Directives have adopted the 'average consumer' norm of law, with significant ramifications for the regulation of B2C private law relationships. The directive having the broadest and most widespread application in the area of consumer law is the UCPD. It prohibits unfair practices at all points in the business-consumer relationship and

[320] Peter Cartwright 'The consumer image within EU law' in Christian Twigg-Flesner (ed) *Research Handbook on EU Consumer and Contract Law*, Cheltenham, Edward Elgar Publishing Limited, 2016, 199.
[321] Dalgaard Laustsen, The Average Consumer in Confusion-based Disputes in European Trademark Law and Similar Fictions, Switzerland, Springer Nature AG, 2020, 6.

is generally applicable to all consumer transactions in the EU. In other words, it applies to all phases of that partnership, including pre-contractual negotiations, advertising, and later information provided in a long-term B2C relationship. Despite its limits, its regime has an impact on a wide range of consumer transactions and company consumer marketing in Europe.[322]

Although it is appropriate to protect all consumers from deceptive business practices, the CJEU has determined that in deciding advertising cases since the passage of Directive 84/450/EEC, it is also necessary to consider the impact on a notional, typical consumer. This Directive adopts the average consumer as a benchmark who is reasonably informed, reasonably observant, and reasonably circumspect, taking into account social, cultural, and linguistic factors, as interpreted by the CJEU, following the principle of proportionality and to enable the effective application of the protections contained in it. However, it also contains provisions meant to prevent the exploitation of consumers whose characteristics make them particularly vulnerable. When a commercial practice is targeted specifically at a certain consumer group, such as children, it is preferable to evaluate the impact of the commercial practice from the viewpoint of the average consumer within that group. As a result, it is appropriate to add a provision that shields children from overt sales pitches without outright banning advertising to children to the list of behaviours that are always unfair. The test of the average consumer is not a statistical analysis. To ascertain the typical response of the average consumer in a particular case, national courts and authorities will need to use their capabilities of judgement while taking the CJEU's case law into consideration.[323]

The concept of the 'average consumer benchmark' was always on the agenda of the EU case law interpretations, even though the definition of 'consumer' in Directive 93/13/EEC was recognised as 'means any natural person who, in contracts covered by this Directive, is acting for purposes which are outside of his trade, business, or profession.'(Art.2)[324] In the *Gut Springenheide* (C-210/96) case while determining 'the average consumer benchmark,' the Court was asked to assess whether statements designed to promote sales are likely to mislead the purchaser, must the actual expectations of the consumers to whom they are

[322] Vanessa Mak, The 'Average Consumer' of EU Law in Domestic Litigation: Examples from Consumer Credit and Investment Cases, *Legal Studies Research Paper Series,* No. 004/2012, Tilburg Law School, 2012, 4-10.
[323] Directive 2005/29/EC, OJ L 149, Rec.18.
[324] Council Directive 93/13/EEC, OJ L 95, Art.2.

addressed, and if it was consumers' actual expectations that mattered, which one - the view of the informed average consumer or that of the casual consumer would be tested. In answering those questions, it should first be noted that provisions similar, intended to prevent consumers from being misled, also appeared in several pieces of secondary legislation and in several cases in which the CJEU has had to consider whether a description, trade mark or promotional text was misleading. In those cases, to determine whether the description, trade mark or promotional description or statement in question was liable to mislead the purchaser, the Court took into account the presumed expectations of an average consumer who is reasonably well-informed and reasonably observant and circumspect.[325]

Thus, as seen from the interpretation of the CJEU's case law, the average consumer is considered to be *reasonably well-informed, reasonably observant and circumspect.* So, here the consumer's level of knowledge is related to the attribute of being informed in the first place. Independent of the information given by a merchant in a specific instance, it refers to the knowledge the consumer possesses or is anticipated to possess. It is impossible to determine if the CJEU has high or low expectations of the consumer in this regard given how little advice can be found in the CJEU's case law in this area. Being informed refers to the consumer's level of knowledge, whereas being observant refers to the consumer's level of observance and information intake. It has to do with the inquiry of how attentive the consumer is to the information offered by the trader. In general, it may be claimed that the CJEU mainly anticipates that the consumer would analyse the facts at hand and make informed decisions. Being circumspect, as the final quality, refers to the consumer's level of scepticism towards the traders' communications. Therefore, being circumspect refers to the processing of this information, or how the consumer deals with the information, and the choice of what to do with it.[326]

The approach embraced by the CJEU reflects the concept 'homo economicus' defined by classical economics: 'an ideal and perfect consumer, who understands what is best for him, acts wisely and consistently, weighs carefully all possibilities available and makes the best decision to suit his interests.' The CJEU expects consumers to make thoughtful and logical

[325] *Gut Springenheide and Tusky v Oberkreisdirektor des Kreises Steinfurts,* C-210/96, Judgment of the Court (Fifth Chamber) of 16 July 1998, para. 15, 28-30.
[326] Bram Benjamin Duivenvoorde, 'The consumer benchmarks in the Unfair Commercial Practices Directive Thesis', *Digital Academic Repository,* Universiteit van Amsterdam, 2014, 67-68.

decisions without taking into account their backgrounds and aiming for a 'one size fits all' type of approach. Abstractly speaking, there is no issue with the CJEU's position since consumers should be responsible for some of their protection. But specifically, it disregards the vast majority of consumer behaviour studies that show that individuals frequently make mistakes, predictably, and do not always encounter a cognitive decision-making process by assessing benefits and drawbacks.[327]

The average consumer covered by the UCPD is, in any case, not someone who only requires a minimal level of protection since they are always in a position to obtain the information that is available and makes informed decisions. Contrarily, as noted in Rec.18, the test is grounded in the proportionality principle. The UCPD adopted the concept to strike the right balance between the need to protect consumers and the promotion of free trade in a market that is highly competitive. As a result, the UCPD's definition of the 'average consumer' should always be interpreted in light of Art.114 of the Treaty, which offers a high level of consumer protection. The UCPD is based on the notion that, for example, a national measure banning claims that might only mislead a very gullible, naive, or superficial consumer (such as 'puffery') would be disproportionate and erect an unjustified trade barrier. The average consumer test is not a statistical test, as Rec.18 makes clear. This means that it should be possible for national authorities and courts to determine whether a practice has the potential to deceive the average consumer. When the interests of particular consumer groups are at stake, the average consumer test is further refined under Art.5(2)(b) of the UCPD. When a practice targets a specific consumer demographic, its effects should be evaluated from the viewpoint of the typical member of the target demographic. For instance, this might occur when a business practice involves a unique product that is advertised through marketing channels to target a limited and specific audience, such as a particular profession. In this instance, the average consumer may not necessarily have more specialised knowledge or characteristics than the average member of that particular group, which has a direct bearing on the evaluation of the effects of the commercial practice. The *particular group of consumers* should be sufficiently identifiable, have a narrow scope, and be homogeneous given the distinction from the general category of the average consumer. The assessment should

[327] Cătălin Gabriel Stănescu, The Responsible Consumer in the Digital Age: On the Conceptual Shift from 'Average' to 'Responsible' Consumer and the Inadequacy of the 'Information Paradigm' in Consumer Financial Protection, *Tilburg Law Review*, vol.24(1), 2019, 53.

concentrate on the benchmark for the general average consumer if a specific group cannot be identified.[328]

The application of the average consumer standard in substantive consumer law, however, raises several questions. First of all, it categorises consumers into the strong and the weak, and it paints the need for more consumer protection as a sign of weakness. Some consumers can be reluctant to declare themselves vulnerable for the sake of receiving protection. Furthermore, unless they can be classified as vulnerable, all consumers who are below average are left without protection under that rule under this approach. They may not necessarily require protection, though. The average consumer falls somewhere along a continuum between protecting all consumers and not protecting any consumers. The average standard may not always accurately reflect the appropriate amount of protection. Moreover, it is quite arbitrary to determine the average standard. Different calculations can indeed be used to determine the average standard. Furthermore, even if it were justified to separate consumer protection from that of the vulnerable, the idea of the typical consumer as 'a reasonably well informed, reasonably observant, and reasonably circumspect' person does not accurately reflect actual consumer behaviour. The typical consumer under EU rules could be described as careful or prudent. In some circumstances, the EU legislation does provide protection for those who are vulnerable, however, it is unclear how severe the vulnerability must be and whether all types of vulnerability are covered. In conclusion, the decision to use the average consumer as the benchmark for protection has not been clearly explained and justified. Even though the average consumer is the one who is utilised to determine the proper level of protection, it is difficult to determine who that average consumer is by experimentation. The idea that consumers should be given more room to protect themselves underlies some of the statements made by courts and legislators.[329]

3.3.2. The vulnerability as a concept in the general understanding

[328] Commission Notice, 'Guidance on the interpretation and application of Directive 2005/29/EC', C/2021/9320 OJ C 526, 33-34.
[329] Geraint Howells, Christian Twigg-Flesner & Thomas Wilhelmsson, *Rethinking EU Consumer Law,* New York, Routledge, 2018, 28-30.

The Latin verb 'vulnerare' - to wound - is where the word 'vulnerable' originates. A vulnerable person is typically understood to be someone who requires extra protection, care, or support or who is in danger of being harmed or neglected.[330] In political sciences, the word 'vulnerability' first appeared, and Professor Fineman's contributions to this field have been particularly significant. According to *Fineman*, the word 'vulnerable' has the power to describe a common, unavoidable, and enduring aspect of the human condition that must be at the core of our understanding of social and governmental responsibility. Thus, liberated from its constrained and unfavourable associations, vulnerability is a potent conceptual tool that has the potential to define the state's obligation to ensure a richer and more substantial guarantee of equality than is currently provided by the equal protection model.[331]

The term 'vulnerability' has become widely used in many fields, including sociology, marketing, law, and, most notably, consumer protection. Vulnerability is a complicated and multifaceted concept that is frequently used but not always fully understood in any discipline. It is inherently very challenging to define. All consumers will experience vulnerabilities, according to the literature. As a result, vulnerability is a constant, universal experience that can always be made visible by our unique situations or embeddedness.[332]

Vulnerability can take many different forms and be either temporary, sporadic, or permanent. Since the situation is fluid, businesses must respond in a flexible, specialised manner. The clear message is that we can all become vulnerable. However, many people in vulnerable situations would not identify themselves as 'vulnerable.' The vulnerability has more to do than just the consumer's situation. The actions or procedures of businesses may contribute to it or make it worse. The impact of the vulnerability is significant, and many people are attempting to deal with challenging circumstances and a lack of available resources, energy, and time. Stress can have an impact on mental health and the capacity for effective management.[333]

---

[330] Mary O'Hara 'Foreword' in Christine Riefa and Séverine Saintier(eds) *Vulnerable Consumers and the Law: Consumer Protection and Access to Justice*, Routledge, Oxon, 2021, xiv.
[331] Martha Albertson Fineman, 'The vulnerable subject: Anchoring equality in the human condition' *Yale Journal of Law & Feminism*, vol.20:1, 2008, 8.
[332] Christine Riefa & Séverine Saintier 'In search of (access to) justice for vulnerable consumers' in Christine Riefa and Séverine Saintier(eds) *Vulnerable Consumers and the Law: Consumer Protection and Access to Justice*, Oxon, Routledge, 2021, 7.
[333] Financial Conduct Authority, Occasional Paper No 8: Consumer Vulnerability, London, 2015, 6-8.

There is a huge volume of academic literature that uses the word 'vulnerability' in a variety of contexts. Generally speaking, it can be interpreted as referring to an *ex-ante* assessment of the likelihood of a potentially bad outcome. When this idea is applied to consumer policy, the vulnerability would therefore be understood to refer to a potentially adverse effect on consumer welfare. In academic and grey literature, a variety of definitions of consumer vulnerability are used. They can be broken down into two main categories: a) definitions that concentrate on the individual characteristics of the consumer, and b) definitions that are more inclusive and take into account the context in which the consumer finds themselves.[334]

According to *Burden*, vulnerability is the inability to obtain or comprehend the knowledge necessary to make decisions about goods and services, as well as the loss of welfare brought on by the purchase of inappropriate goods or services or the failure to purchase appropriate goods and services.[335]

The strategy of identifying certain groups of vulnerable users has come under fire from more recent critical advancements in the vulnerability literature for being unduly patronising and detached from social realities. *Fineman*, with her vulnerability theory, is one of the most well-known and effective proponents of an alternate strategy for dealing with vulnerability. As a result of human embodiment, which brings with it 'the ever-present risk of pain, injury, and disaster,' vulnerability is a result that 'no one can avoid,' claimed *Fineman*.[336]

It is critical to stress right away that vulnerability is a complicated idea. It covers a wide range of traits that can be either permanent or temporary and range in severity. Additionally, vulnerabilities rarely fit neatly into predefined categories. Each individual will experience some aspects of a vulnerability to varying degrees and frequently in overlapping ways. To consider how vulnerability can impact a customer's interaction with the energy market, some general categories can be used. The initial type is financial vulnerability, which means that the income of a large number of clients is not enough to pay for their household expenses. Different nations have different ideas about what this phrase means. However, it broadly

[334] European Commission, 'Consumer vulnerability across key markets in the European Union: Final report', Luxembourg, Publications Office of the European Union, 2016, 41-42.
[335] Ramil Burden, 'Vulnerable consumer groups: quantification and analysis' *OFT Research paper,* vol.15, 1998, 61.
[336] Fineman, The vulnerable subject, 8.

refers to a situation where customers are unable to afford to heat their homes adequately. There is vulnerability due to health and capacity issues: this can include those who suffer from hearing loss, vision impairment, physical disabilities, illiteracy, digital illiteracy, a poor understanding of the local language, and poor mental health. The last category is a location-based vulnerability in which residents of remote, rural areas might only have a small selection of energy providers. Additionally, the older age of rural properties combined with rural areas' lower average wages can raise the risk of fuel poverty. Vulnerability can frequently be sporadic or a transitory stage, both within and outside of these categories. A sudden change in circumstances, such as being laid off or having a variable income, can leave one vulnerable financially. A short-term illness or death can lead to temporary vulnerability. This could imply that anyone, at any time, is just a moment away from turning into a client who would be regarded as vulnerable. [337]

Starting with sources of vulnerability, there are two types: inherent sources and situational sources. Inherent sources that are inherent to the human situation and 'arise from our corporeality, our neediness, our dependence on others, and our emotive and social natures' are corporeality, neediness, and dependency on others. Situational vulnerabilities, on the other hand, are those that only appear in specific circumstances or situations and are not inherent characteristics of human nature. Vulnerabilities can be caused by or made worse by a range of influences of various kinds, including personal, societal, political, or environmental effects. Together with what causes vulnerabilities, the matter of how vulnerabilities can present themselves should also be addressed. This is where the various vulnerability states - which might be dispositional and occurrent - come into play. Vulnerabilities can be dispositional and occurrent, whether they are situational or inherent. Potential vulnerabilities are roughly what the category of dispositional vulnerabilities refers to. To put it another way, dispositional vulnerabilities are those flaws that have not yet shown themselves but may if certain conditions were present - in this case, all the previously mentioned inherent and situational sources. Those dispositional vulnerabilities that additionally exhibit themselves are referred to as occurrent vulnerabilities in this context.[338]

[337] Commission for Customers in Vulnerable Circumstances, 'Final Report 2019', 2019, 19-20.
[338] Natali Helberger et al., *EU Consumer Protection 2.0: Structural asymmetries in digital consumer markets*, Brussels, 2021, 16-17.

3.3.3. The concept of vulnerable consumers in the general understanding

A lot of consumer protection legislation is based on the idea of the average or typical consumer and what that consumer might anticipate, comprehend, or act. Consumers in vulnerable situations, however, might be much less able to advocate for their interests and more likely to experience harm than the typical consumer.[339]

Sometimes consumers will be so helpless as to lack capacity, so the law must make allowances for such situations. There is disagreement over whether to label these consumers as disadvantaged or vulnerable. A disadvantaged consumer is defined as a person in persistent circumstances and/or with ongoing attributes which adversely affect consumption thereby causing a continuing susceptibility to the detriment of consumption. A vulnerable consumer is capable of readily or quickly suffering detriment in the process of consumption. This definition of vulnerability is very broad; even though most consumers are in a good position to make wise decisions, many consumers are capable of experiencing harm quickly or readily.[340]

In the early 1970s, consumer vulnerability was at the centre of EU consumer law since consumers were seen as the weaker party due to their status. Therefore, all consumers were viewed as being vulnerable in the early days of consumer law. Before the creation of consumer law, there were also remedies for parties in a weaker position in contract law and private law more generally, and those have persisted concurrently. The way this group was perceived to have fragmented as consumer law evolved, with the 'average consumer' standard emerging as the de facto benchmark. It is true that consumers are no longer thought of as a homogenous group and that some require a higher level of protection than others. This is confirmed by the more recent recognition of consumer 'vulnerability.' Despite the rising interest in consumer vulnerability, no single definition is universally acknowledged.[341]

According to *Andreasen et al.*, vulnerable consumers are those who 'face disadvantages in exchange relationships where those disadvantages are attributable to characteristics that are

[339] Financial Conduct Authority, 'Occasional Paper No 8', 6-8.
[340] Peter Cartwright, 'Understanding and protecting vulnerable financial consumers' *Journal of Consumer Policy*, vol:38(2), 2015, 119-138.
[341] Eleni Kaprou 'The legal definition of 'vulnerable' consumers in the UCPD: Benefits and limitations of a focus on personal attributes' in Christine Riefa and Séverine Saintier (eds) *Vulnerable Consumers and the Law: Consumer Protection and Access to Justice*, Oxon, Routledge, 2021, 51.

largely beyond their control.'[342] Another significant component of more recent definitions of consumer vulnerability is the idea that it is a dynamic term. *Griffiths and Kizer* acknowledged that customers may enter and exit circumstances where they are exposed to danger or are vulnerable for a certain amount of time. The risk and transitory condition of vulnerability vanish when the situation does.[343]

Consumer law establishes several standards, guiding principles, and institutions of protection in their favour in recognition of the structural vulnerability of consumers in the market in their interactions with suppliers of goods and services. The impact of information and communications technologies on business has particularly emphasised this structural vulnerability. The unnaturalness of the technological event, the supplier's control over electronic media, and a higher propensity to risks related to security and self-determination in terms of personal data, payment methods, breach of trust, fraud, and trademark fraud, among others, all contribute to the consumers' vulnerability in mass consumption, which is depersonalised and globalised.[344]

Consumer vulnerability is a concept that is frequently used by other disciplines, most notably marketing and is not just a legal concept. As a result, the literature from various academic fields accurately reflects the advancements in the theory of consumer vulnerability. In law and other disciplines, a clear definition of consumer vulnerability has proven elusive. The way that consumer vulnerability is conceptualised has also significantly changed over time. The biggest shift has been from seeing certain consumer groups as completely vulnerable (what is commonly referred to as a 'class-based' approach), like the elderly or women, to seeing vulnerability more and more as a transient state (what is commonly referred to as a 'state-based' approach). According to the class approach, vulnerable consumer groups include the underprivileged and the illiterate. A class approach frequently overlooks the various market-related and other factors that affect consumer vulnerability. This could exacerbate stigmatisation and exclusion of groups that are considered vulnerable. However, it has the vital benefit of making it clear who is regarded as vulnerable. This is crucial in the

[342] Alan R. Andreasen et al., 'The Dissatisfaction and Complaining Behavior of Vulnerable Consumers' *The Journal of Consumer Satisfaction, Dissatisfaction and Complaining Behavior,* vol.3, 1990, 13.
[343] Merlyn Griffiths & Tracy Harmon-Kizer, 'Aging Consumer Vulnerabilities Influencing Factors of Acquiescence to Informed Consent' *Journal of Consumer Affairs*, vol.45/3, 2011, 445-466.
[344] Sergio Sebastián Barocelli 'Consumer Protection and Sharing Economy' in D. Wei et al. (eds.*), Innovation and the Transformation of Consumer Law*, Singapore, Springer Nature Pte Ltd., 2020, 19.

legal context, where a priority may be given to certainty. According to some authors, state-based vulnerability refers to consumer vulnerability as the result of the interaction of numerous factors, including both external and internal states and characteristics. The authors made the case that when these factors interact, the consumer is rendered helpless, and it is this result that determines whether or not the consumer is in a vulnerable position. This more impartial method helps eliminate the stigmatisation of particular social groups. It enables decision-makers to take vulnerability against shifting social conditions into account. This strategy highlights that consumers can overcome their vulnerability and enables a wide range of factors to be taken into account.[345]

Many situations might lead to vulnerability. According to one taxonomy, consumers may be more vulnerable due to factors such as a) information vulnerability, which is related to the ability to receive and comprehend information or to make the best decision; b) pressure vulnerability, which refers to a higher susceptibility to hard pressure selling techniques; c) supply vulnerability, which constitutes an inability to afford essential goods or services, or limited choice within an affordable price range; d) redress vulnerability which is the inability to obtain redress for wrongs committed and e) impact vulnerability which is more adversely impacted by poor decisions.[346]

3.3.4. Vulnerable consumers in the EU consumer protection law

The concept of the 'vulnerable consumer' has been incorporated into EU policy. In addition to addressing consumer vulnerabilities generally, EU consumer law occasionally acknowledges that some consumers are more vulnerable than others and as a result, need extra protection or tools for empowerment. In comparison to an approach based on the benchmark of the typical consumer, the recognition advances a new method of evaluating B2C transactions. Initially, even though consumer law generally applies to all consumers, protections for those who are vulnerable only apply to a subset of consumers, or more specifically, the unique vulnerability of some consumers necessitates a different evaluation of the parties' conduct. The vulnerability concept invites us to evaluate the impact of measures

[345] Kaprou, 'The legal definition of 'vulnerable' consumers in the UCPD', 54.
[346] Nikolina Šajn 'Vulnerable Consumers Summary' *EPRS/European Parliamentary Research Service*, 2021, 3.

on various consumer groups. While consumer law is typically mandatory, meaning that consumers cannot opt out of consumer protection even if they do not benefit from it, this is contrary to the vulnerability concept. For instance, certain consumer practices might only be prohibited if the vulnerable consumers who are the target would otherwise suffer a significant loss.[347]

The critical consumer law literature also raises concerns about the excessively static and stigmatising impacts of a non-universal approach to consumer vulnerability. Legal scholars have criticised this situation for presenting consumer protection law as something that only the 'weak' require and for the rigidity of the divide between the average and vulnerable consumer. Perhaps adding to these worries is the digitalisation of consumer markets. In other words, neither the average consumer nor the vulnerable consumer is any longer the exception. It is interesting to note that in more recent policy documents from the European Commission, there has been a gradual trend towards this more global perspective on vulnerability and an effort to do away with the rigid, categorical definition. The two primary points of view in the consumer research literature on vulnerability are caused by disadvantages and marketer manipulation. In terms of disadvantages, the research in this field focuses on those who are less fortunate due to their unique traits, socio-economic circumstances, and access to resources. Researchers have studied how and why interpersonal interaction can make people more susceptible to marketing fraud, for instance, in the context of manipulation. Others have noted that these people are not so much vulnerable because they belong to a certain type of consumer, but rather because of the situations they find themselves in. So, in terms of the thinking on vulnerability theory going forward, a significant contribution of recent theoretical breakthroughs is the awareness that vulnerability is a universal condition rather than an exceptional one reserved for specific consumer groups.[348]

Regarding the variation of vulnerability incidence rates within the EU, the countries where the vulnerability incidence rates are generally significantly lower are Germany, the Netherlands and Norway, while the opposite is true for Cyprus, and a little lower in Croatia and Romania. For the majority of the vulnerability indicators, the incidence of vulnerability tends to be higher in the energy and financial sectors than in the online sector among the three

[347] Jule Mulder, 'Comparing Vulnerability? How can EU comparative law methods shed light on the concept of the vulnerable consumer' *Journal of International and Comparative Law (JICL)*, vol.6(2), 2019, 209–231.
[348] Helberger et al., *EU Consumer Protection 2.0*, 10-13.

sectors of specific relevance for the study. But each of the areas has crucial distinctions. Complexity creates a barrier for a very wide variety of consumers, especially in the financial and energy industries, as they are likely to find it challenging to grasp and compare offers. The Report on consumer vulnerability in the EU sought to operationalize consumer vulnerability in terms of a set of five factors based on the available literature. This operationalisation can then be utilised to improve and modernise the vulnerability definitions that already exist. So, one possible definition of a 'vulnerable consumer' is a consumer who, as a result of sociodemographic factors, behavioural features, personal circumstances, or market environment a) is more likely to experience unfavourable market outcomes; b) is unable to fully maximise their well-being; c) has trouble gathering or absorbing information; d) has a harder time finding, choosing, or purchasing appropriate products; or e) is more vulnerable to specific marketing techniques.[349]

The European Parliament introduced the resolution of May 22, 2012, on a strategy for strengthening the rights of vulnerable consumers to promote consumer rights and their protection as core values for developing pertinent EU policies, particularly for strengthening the single market. The European Parliament noted that a uniform approach and the adoption of a comprehensive legislative instrument are hampered by the variety of vulnerable situations, both when consumers are subject to statutory protection and when they are in a particular situation of sectoral or temporary vulnerability. Because of this, the issue of consumer vulnerability must be addressed by European law as a horizontal task, taking into account the diverse needs, capacities, and circumstances of consumers, and the MS must adopt the necessary actions to provide adequate guarantees for the protection of vulnerable consumers. The issue of consumer vulnerability was first addressed in EU legislation in Directive 2005/29/EC, which established a concept of vulnerability tailored to said practices and focused on 'undue influence' that could be exerted over consumers whose volition was not fully formed. The UCPD on the other hand, only protected consumers' economic interests and did not cover other possible areas such as their health, safety, or even moral integrity. Because of the complexities of applying a static definition to each of the various vulnerable situations that can affect consumers throughout their lives, European legislation and policies have addressed the issue of vulnerability on a case-by-case basis up to the present time. In

[349] European Commission, 'Consumer vulnerability across key markets in the European Union', xix-xx.

other words, political and legislative instruments aimed at mitigating or preventing vulnerability tend to focus on a single vulnerability factor.[350]

The CRD also makes mention of more vulnerable customers. The CRD's Rec.34 states that before the consumer is bound by a distance or off-premises contract, a contract other than a distance or off-premises contract, or any related offer, the trader must provide the consumer with clear and understandable information. The trader should consider the particular needs of consumers who are especially vulnerable due to their age, credulity, or mental, physical, or psychological impairment when delivering that information, as the trader could reasonably be anticipated to foresee. Therefore, differing levels of consumer protection shouldn't result from taking into consideration such unique needs.[351]

Despite directly addressing vulnerable customers, the UCTD stipulates in its recitals that 'in formulating a judgement of good faith, particular reference shall be taken to the strength of the parties' bargaining positions.'[352] The European Commission's guidance on the UCTD also implies that the viewpoint of more vulnerable consumers should be considered when analysing the potential effects of certain barriers on consumers' ability to pursue remedies or the potential effects of restricted knowledge and information in this regard. Even in cases when the contract provisions used against them are visibly unjust, such consumers may be especially hesitant to pursue the available remedies.[353]

The Directive 2001/95/EC on general product safety also recommends that when evaluating a product's safety, all pertinent factors be taken into consideration, particularly the consumer groups that may be particularly vulnerable to the risks that the product in question poses, such as children and the elderly. In addition, Art.2(b) states that products could be deemed unsafe if they are not safe for consumer groups who are at risk when using them, particularly children and the elderly.[354] Art.5 of the Regulation (EU) No 524/2013 on Online

[350] María Irigoyen Pérez, 'Report on a strategy for strengthening the rights of vulnerable consumers' *Committee on the Internal Market and Consumer Protection,* European Parliament 2009-2014: Plenary sitting, A7-0155/2012, 8.5.2012, 6/15.
[351] Directive 2011/83/EU, OJ L 304, Rec.34.
[352] Council Directive 93/13/EEC, OJ L 95, 29-34.
[353] Commission Notice, 'Guidance on the interpretation and application of Council Directive 93/13/EEC on unfair terms in consumer contract (Text with EEA relevance)' OJC 323, 27.9.2019, 4-92.
[354] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (Text with EEA relevance), OJ L 11, 15.1.2002, 4–17.

Dispute Resolution (ODR) requires that the ODR platform is 'accessible and usable for all, including vulnerable users ('design for all'), as far as possible.'[355]

The European Commission released a new consumer agenda on November 13, 2020, outlining its vision for consumer policy from 2020 to 2025. The Commission intends to strengthen protection for vulnerable populations, particularly children and those without internet access, as one of its five top priorities during the subsequent five time periods. The most relative agenda priorities for topics related to vulnerable consumers are the problems of accessibility, financial vulnerability and products for children.[356]

3.3.5. Vulnerable consumers in the UCPD

The information paradigm is the basis of the UCPD: by ensuring a flow of accurate and insightful information, transactional decisions made by 'average consumers' are made in an unaltered way and, as a result, can be presumed to be in line with their preferences. The UCPD is characteristic of the traditional economic framework of EU consumer policy from this angle. The UCPD varies between two goals, empowering self-sufficient and autonomous consumers, particularly average consumers and protecting vulnerable average consumers. Regarding the first goal, the Directive adheres to the information paradigm, which strengthens autonomy and places a focus on individual responsibility. On the other hand, the Directive succeeds in defending consumers generally, and particularly vulnerable consumers, against businesses that prey on their superior understanding of consumer behaviour and flaws in people.[357]

Under Art.5(3) of the UCPD, commercial practices which are likely to materially distort the economic behaviour only of an identifiable group of consumers who are particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity in a way which the trader could reasonably be expected to foresee,

[355] Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR) OJ L 165, 18.6.2013, 1–12.
[356] Nikolina Šajn, 'New consumer agenda: Summary' EPRS/ European Parliamentary Research Service, Members' Research Service, PE 679.079, 2021, 1.
[357] Willem H van Boom 'Unfair commercial practices' in Christian Twigg-Flesner (ed) *Research Handbook on EU Consumer and Contract Law*, Cheltenham, Edward Elgar Publishing Limited, 2016, 402-403.

should be assessed from the perspective of the average member of that group. This does not interfere with the typical and acceptable practice of using statements that shouldn't be taken literally in advertising. Rec.19 of the UCPD made clear that in cases where a consumer's age, physical or mental infirmity, or credulity make them particularly susceptible to a commercial practice or to the underlying product, and only those consumers' economic behaviour is likely to be distorted by the practice in a way that the trader can reasonably foresee, it is appropriate to ensure that they are adequately protected by evaluating the practice from the perspective of the average member of that group.[358]

Most consumers display signs of vulnerability in at least one area, while a third exhibit indication of vulnerability in many dimensions, according to the UCPD's Guidelines. The influence of personality traits on the chance of becoming a susceptible consumer is as multifaceted as consumer vulnerability itself. It would be appropriate to evaluate a commercial practice from the perspectives of consumers of different ages when it comes to age. Depending on their age and developmental stage, children's capacities for comprehending both online and offline advertising will differ substantially from one child to the next. Due to their advanced age, elderly persons may be more susceptible to some behaviours. Although aggressive door-to-door sales tactics may not have an impact on the average consumer, nevertheless it is likely to frighten some consumers, especially the elderly who may be more susceptible to pressure sales. Physical or mental infirmity can cause sensory impairment, reduced mobility, and other problems. The term 'credulity' refers to a subset of consumers who may be more likely to trust certain promises. The term is contextual and impartial, therefore its impact is to safeguard group members who are, for whatever reason, more susceptible to being swayed by a particular business technique. If a commercial practice alters the economic behaviour of a group of consumers who are particularly vulnerable 'in a way that the trader could fairly be expected to foresee,' then the 'vulnerable consumer' criteria apply. This criterion adds a proportionality component to the evaluation of commercial practices concerning vulnerable consumers. It tries to hold business owners accountable only

[358] Directive 2005/29/EC, OJ L 149, 22–39.

when the harm caused by a business practice on a group of particularly vulnerable consumers may be reasonably foreseeable by the trader.[359]

The term 'vulnerability' encompasses context-dependent weaknesses in addition to the traits stated in Art.5(3). In the digital environment, which is increasingly characterised by data collection on socio-demographic characteristics as well as personal or psychological characteristics, such as interests, preferences, psychological profile, and mood, multidimensional forms of vulnerability are particularly acute. Art.5(3) appears to only define consumers as vulnerable because of their 'mental or physical infirmity, age, or credulity.' However, Rec.19 of the Preamble includes a non-exhaustive list of traits that render a consumer 'particularly susceptible.'[360]

The country-based study used for the Fitness Check led to the following results on vulnerable consumers. The vulnerable consumer benchmark is regarded as having little practical application, and the benefits of this provision for consumers thus far appear to be largely theoretical. The particular rules of Art.5(3) UCPD for consumers who need greater protection generally do not seem to be applied very often by national courts and enforcement agencies. The relevant authorities and courts' decisions hardly ever refer to Art.5(3) UCPD. The primary justification seems to be that the benchmark for the average consumer was intended to represent the norm, with the vulnerable consumer being the strict exception. Instead of using the 'vulnerable consumer' benchmark stipulated in Art.5(3) UCPD, national courts and enforcement agencies frequently use the 'modulated average consumer standard.'[361]

Although well-intentioned, the average vulnerable consumer was designed, but due to its overly limited scope and stringent requirements, it is not able to adequately protect vulnerable consumers. It has been criticized for excluding other traits, such as education, race, or economic level, which scientific research has shown can lead to vulnerability. The UCPD does not take into account the fact that vulnerability can affect large segments of the consumer

[359] European Commission, 'Commission Staff Working Document Guidance on A comprehensive approach to stimulating cross-border e-Commerce for Europe's citizens and businesses,' 25.5.2016, SWD (2016) 163 final, 43-46.
[360] Commission Notice 'Guidance on the interpretation and application of Directive 2005/29/EC', C/2021/9320 OJC 526, 35-36.
[361] Civic Consulting, 'Study for the Fitness Check of EU consumer and marketing law', Final report Part 1 – Main report, Brussels, European Commission, 2017, 43-44.

population or the idea that everyone can experience vulnerability at some point, treating the average vulnerable standard as an exception.[362]

The tightness of the line between the average consumer and the vulnerable consumer has drawn criticism from legal scholars. The distinction between a vulnerable consumer and the average consumer, however, has become even less useful in protecting consumers from pervasive online commercial practices as the digital environment has developed. In a nutshell, the majority of consumers - if not all - are potentially vulnerable in digital marketplaces. To address this reality, the term 'digital asymmetry' was developed to describe a universal state of defencelessness and susceptibility to the exploitation of power imbalances that arise as a result of rising levels of commerce automation, data-driven relationships between buyers and sellers, and the very structure of digital marketplaces. Some authors argued that the UCPD should adopt the principle of data protection by design and by default found in Art.25 of the GDPR by introducing new concepts like digital asymmetry and digital vulnerability, adapting the idea of transactional decision, imposing a duty of care on traders, and concretizing the general idea of 'fairness by design.' The majority of the experts who were interviewed agreed with this viewpoint and maintained that the UCPD's existing definition of a 'vulnerable consumer' is either insufficient or ineffective in the context of the digital world.[363]

Only a few cases addressing consumer vulnerability were found in the UCPD legal database. Vulnerable groups were identified, including a) consumers barred from credit institutions (*Hungarian case Vj-5/2011/73*); b) those suffering from a serious illness (*Italian case PS6980*); and c) consumers in a particular demographic, such as women between the ages of 40 and 60 (*Italian case PS649*). This in turn implies that several interpretations of consumer vulnerability are used in EU case law, each of which is greatly influenced by the particular market environment. Yet, the initial ruling's partial consideration of consumer vulnerability indicates that it may be difficult to apply this concept in practice. Overall, the small number of instances involving vulnerability indicates that this topic is still largely under-examined in legal contexts throughout MS. It is crucial to consider cases from outside

[362] Kaprou, 'The legal definition of 'vulnerable' consumers in the UCPD', 64.
[363] European Commission, Directorate-General for Justice and Consumers 'Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation' *Final Report*, Brussels, 2022, 91-109.

the EU since national case law has not focused much on consumer vulnerability and the concept of the average consumer.[364]

Some scholars have noted that the existing strategy for dealing with vulnerability under UCPD Art.5 (3) is out of date and not very helpful in addressing the issue of the digital consumer. So, a definition of digital vulnerability would be appropriate for the digital age in some way to reflect the industry's constant pursuit of innovative and creative digital marketing techniques that aim to optimise consumer behaviour patterns.[365]

For this reason, the BEUC recommended that the UCPD recognise digital vulnerability as the universal state of susceptibility to decision-making distortion under circumstances of digital asymmetry, in addition to the current construct of consumer vulnerability based on personality traits and personal characteristics. Digital vulnerability, a global state of susceptibility to the exploitation of power imbalances in the trader-customer interaction as a result of internal and external elements beyond the control of the consumer, is what results for the consumer. Inadequate digital literacy, cognitive biases, or information overload are a few examples of such internal variables. The digitally mediated connection, decision architectures, knowledge gap, limited control over data through user interfaces, design of digital consumer environments and choices, lack of service interoperability, default configuration settings, etc. are examples of external variables.[366]

As follows from Art.5(3), there are some prerequisites for the application of the vulnerable group benchmark. Foremost, to use a vulnerable group of benchmarks, it must be 'identifiable' as the vulnerable group. However, there is no slightly direct indication of what can be considered clearly identifiable and for whom the group can be considered clearly identifiable. Also, as can be seen from the provisions of Art.5(3) 'commercial practices which are likely to materially distort the economic behaviour only of an identifiable group of consumers.' From this wording, it can be assumed that this practice applies only to a certain group of consumers, especially a vulnerable group of consumers, while the other group of consumers remains unaffected. Thus, the role of the vulnerable group of consumers is specified here in comparison with the average and target group of consumers. In that case, the situation becomes more complicated, since the word 'only' includes the economic behaviour

[364] European Commission, 'Consumer vulnerability across key markets in the European Union', 145-146.
[365] Helberger et al., *EU Consumer Protection 2.0*, 15-24.
[366] BEUC, 'BEUC framing response paper for the REFIT consultation', 5-6.

of a vulnerable group of consumers, excluding the average and target group of consumers. However, what about in real cases, when not the elderly, but vulnerable consumers also need the necessary protection compared to the vulnerable group of the benchmark? Neither the UCPD nor the Court considered relative and subsequent actions to find joint solutions to such a situation with possible outcomes for both groups. Even though age is one of the causes of vulnerability, the UCPD does not mention the age period for children and older consumers, who are considered the vulnerable group of the benchmark. Another cause of vulnerability, especially infirmity, was cited too broadly, as it did not establish rules for distinguishing between mental and physical disorders of consumers by merchants when shopping. Thus, as a way out of such situations and to achieve better results, it might be better to take into account the discretion of MS in assessing situations on a case-by-case basis, taking into account all relevant circumstances. In general, it seems that even if all the necessary information and legal concept of the vulnerable consumer benchmark group has been presented, its practical and logical decision-making ability is more inefficient in real-life situations than that of the average consumer benchmark group.

3.3.6. Summary

Inevitably, current consumer regulatory mechanisms are better suited to protect and identify the average group of consumers in a proper position. However, in addition to the average consumer, which is one of the main participants in consumer relations, there is also a certain group of consumers that is more susceptible than the average group of consumers. This group is a vulnerable group of consumers, which is a clearly identifiable group based on mental or physical disability, age or credulity, and the trader can reasonably be expected to 'foresee their vulnerability'.

Regarding the age of the vulnerable consumer group, it would be better to define and set some age groups for both children and elderly consumers. The approach of indicating the extent to which the infirmity is susceptible (whether mental or physical) and the level of credulity would be important to protect the vulnerable group of consumers from misleading commercial practices. Since there are indefinite periods of age, degrees of infirmity and credulity for a particularly vulnerable group of consumers, who can be identified as a clearly

identifiable group, their economic behaviour is significantly distorted. Due to the sensitivity of the vulnerable group of consumers, traders may be compelled to use the average consumer benchmark to avoid unpredictability and confusion with national authorities. As the most vulnerable group of consumers is evaluated from the perspective of the average member of that group, it has become challenging for courts to apply the general standardized rules of the UCPD on a case-by-case basis.

In particular, by using the average consumer group as a benchmark on the consumer protection law, the UCPD is no longer up to date to provide an adequate definition of the vulnerable consumer group that should be consistent with the recent digital transformation. A consistent and coherent approach directly to the establishment of criteria for digital vulnerability should be taken into account as a guide to the use of a vulnerable group of consumers, not only in commercial practices but also in other industries. The position and provision of the vulnerable group of consumers must be effectively adapted to the contemporary issues of the digital single market, especially in light of the rapid growth of information technology. Therefore, it would be more useful and realistic for legal scholars to make further contributions by identifying the characteristics of particularly digitally vulnerable consumer groups and the likelihood of being particularly vulnerable to certain commercial practices.

In an attempt to answer the research questions about the extent to which EU consumer protection law can identify and protect vulnerable consumer groups, here are some of the findings of the study. Regarding the first part of the definition of the vulnerable consumer group, the EU has somehow managed to develop a static fixed definition, but it is formulated only from the point of view of the UCPD. As a result, other consumer-related online industry practices, such as contractual relationships or dispute resolution situations, are not subject to consumer protection laws and policies that take into account, vulnerable consumers.

Despite the initiatives of the EU to specify the definition of vulnerable consumers, this definition itself lacks situational and inherent factors, which, of course, are an integral part of various consumer groups. Another factor behind this definition is that this definition does not represent the actual digital capacity of online consumers or vulnerable consumers, and therefore it cannot show their current value in the digital marketplace. Since there is no established guidance on how traders should determine who belongs to different vulnerable

consumer groups, it will be difficult from a practical point of view to differentiate and protect vulnerable consumer groups, apart from certain factors. As a solution to such a situation, instead of representing the collective interests of consumers, industry individually created representative consumer protection agencies will be more useful in cooperating and monitoring the digital marketplace from the perspective of vulnerable consumers.

Based on the position of EU consumer law, it is assumed that the consumer regulation mechanism in the EU is more suitable for protecting the typical average group of consumers, both in theory and in practice. Despite provisions for vulnerable consumers in EU consumer law, it is practically very difficult for vulnerable consumers to know when they need protection from unfair commercial practices. Since vulnerable groups do not receive reliable information or this is not possible due to extrinsic and intrinsic factors, these vulnerable consumer groups will always need additional guidance and assistance in online transactions.

Chapter 4. The concept of vulnerable individuals in the data protection law

This chapter is going, to begin with, a brief overview to show how the evolution of privacy and data protection law has been driven by technological developments. Later, the various rights of data subjects with relevant court cases will be considered in terms of clarifying the status of data subjects in exercising their rights when processing personal data following the rules of the GDPR. Thus, after the main provisions of the GDPR and the clarification of the fundamental rights of data subjects, average and vulnerable individuals as the data subjects will be examined and analysed in terms of determining the extent to which EU data protection law can define and ensure adequate protection of vulnerable individuals during processing data.

4.1. Online users' privacy and data protection rights and their regulation

Technological developments are fundamentally altering society. Numerous aspects of people's lives are impacted by new technology, including how they interact with others, with businesses, and with the government. Even though technology allows us to complete numerous things more quickly and previously impossible ones, these successes are not free. Although they offer remedies to current issues, numerous technical breakthroughs frequently give rise to brand-new, occasionally unanticipated issues. The issues that these innovations raise must be addressed, as society adapts to them for technological advantages to exceed their drawbacks. The right to privacy is one area where modern technology is currently causing such issues.[367]

The EU Charter (Art.7) made a brief statement on privacy, noting that 'everyone has the right to respect for his or her private and family life, home and communications.' The EU Charter also distinguished the right to the protection of personal data by citing that 'everyone has the right to the protection of personal data concerning him or her.'[368] Legally speaking, privacy and data protection are two separate fundamental rights under the EU law, with the first being a substantive right that is created to ensure the protection and promotion of human

[367] Thomas B. Kearns, 'Technology and the Right to Privacy: The Convergence of Surveillance and Information Privacy Concerns' *William & Mary Bill of Rights Journal*, 1999, 975-976.
[368] Charter of Fundamental Rights, Art.7.

interests as well as those of society, and the second being a procedural right that establishes the guidelines, procedures, and frameworks necessary for the effective enforcement and protection of substantive rights.[369]

In many ways, privacy is a topic where companies and people frequently have divergent goals. For instance, in e-commerce, consumers want their information to be used only as needed to complete the transaction, but businesses frequently want to profit from the consumer data they collect.[370] This information is either required for the transaction (e. g., credit card information) or desired by the e-commerce as having it allows them to analyse it, find trends, and improve the effectiveness of their business dealings. Users frequently lack awareness of the variety of potential applications that possessing this information permits, and as a result, lack awareness of the potential privacy violations that might take place right in front of them with their inadvertent assent. However, in the modern world of the information age and e-commerce, there appears to be a need for and potential of reaching a compromise between the two opposing concepts and arriving at a solution that is advantageous to all parties. To enable the ability of the individual to keep the greatest level of privacy and control over their personal information, this compromise supports user-centric privacy in e-commerce.[371]

Information privacy and personal privacy are the two main divisions of privacy. The methods used to collect, record, access, and release information are referred to as information privacy. Personal privacy refers to a person's privacy, or their personal space, which might be 'invaded' by people who want to take pictures, record videos, or record audio in both public and private settings.[372]

In addition to being a collection of legal rules outlined in a legal text, privacy is also first and foremost a set of social norms that are universally accepted and followed by both the consumer and the trader. The main issue underlying privacy is that how commerce has been digitised represents a radical shift in a social privacy consensus between consumers and

[369] E. Politou et al., *Privacy and Data Protection Challenges in the Distributed Era*, Switzerland, Springer Nature AG, 2022, 9-10.
[370] France Bélanger & Robert E. Crossler, 'Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems' *MIS Quarterly*, vol.35/ 4, 2011, 1017-1041.
[371] Rhys Smith & Jianhua Shao, 'Privacy and e-commerce: a consumer-centric perspective' *Electron Commerce Research*, 2007, vol.7, 101.
[372] Davidson, The law of e-commerce, 218.

merchants. Even if this was not the merchants' original, deliberate, or conscious intention, the technology that the Internet industry has widely implemented is radically altering, at least in terms of privacy, the socially accepted way in which customers and commercial companies exchange and share personal information.[373]

Businesses should not consider managing privacy to be a burden. Instead, it might be a useful strategy for developing and preserving a strong bond with your consumers. Establishing a framework for consumer privacy controls should be seen by businesses as a crucial marketing and strategic component that offers significant advantages. Companies can use one of three methods to turn touch points involving privacy into a satisfying consumer experience. The opening method is to create user-centric privacy settings to provide users with power. This idea of managing privacy transcends the too-basic conceptions of data privacy that have dominated most of the political discussion surrounding online privacy. The idea of a global opt-in or opt-out mechanism in which users can decide to control businesses' tracking of their online movements has received a lot of attention in this debate. The next method is multiple intrusion prevention since a critical component of privacy is the ability to repel unauthorized intrusion. Due to technology, companies seem to be able to breach user privacy in several ways. The last method is, where possible, to use automation to prevent human intrusion. When a machine analyses personal data rather than a person, users are more at ease.[374]

The utilisation of personal data is a vital component of the digital economy. As a key input, personal data is being used by a growing number of business models. Users receive tailored and cutting-edge services in return for contributing their data. At the same time, concerns about privacy and fundamental rights are raised by businesses' acquisition, processing, and use of personal data. Furthermore, given the significant strategic and commercial worth of personal data, its collection, management, and usage may cause competition issues and harm consumers. The management of personal data can be impacted and, thus, directly and indirectly, regulated by various disciplines of law, such as competition

[373] Ien Walden & Julia Hornle, *E-commerce law and practice in Europe*, Cambridge, Woodhead publishing editing Limited, 2001, ch.2, 19.
[374] Avi Goldfarb & Catherine Tucker, 'Why Managing Consumer Privacy Can Be an Opportunity' *MIT Sloan Management Review,* Special Collection: The Fine Line Between Service and Privacy, 2017, 1-3.

law, unfair competition law, consumer protection legislation, and IP law, in addition to being subject to the application of the data protection standards.[375]

Data protection cannot be encapsulated in two or three lines. The word 'data protection' refers to a broad range of concepts relating to the handling of personal data. Governments attempt to reconcile essential but incompatible principles such as privacy, the free flow of information, the necessity of governmental surveillance, the imposition of taxes, etc. by using these concepts. In contrast to criminal law, data protection generally lacks a restrictive element. Data is not owned by data subjects. They frequently can't stop the processing of their data. Currently, data controllers - actors who handle personal data - have the authority to handle other people's data as well. Since the use of personal information is frequently required for social reasons, data protection is therefore pragmatic and presupposes that both private and public actors must be able to utilise it. The data protection laws protect us from disproportionate or illegal processing of data, not from data processing itself.[376]

Following the constitutional enshrinement of a right to data protection at the EU level, much effort has been directed towards defining the precise nature of the link between privacy and data protection. The topic of whether data protection may be thought of as a 'separate' or 'independent' basic right, 'different' from the right to privacy, or whether it can be seen as merely a component of privacy, is the subject of a heated dispute among the EU scholars. Foremost, it is important to remember that data protection and privacy are both fundamental rights recognised by the EU Charter, which serves as the foundation of EU law. This indicates that data protection is thought to or is anticipated to add something to privacy, at least within the context of EU constitutional law. Moreover, it is worthwhile not to lose sight of the historical fact that data protection laws are very recent, having only come into existence in the 1970s in response to worries about the development of enormous data banks and the more centralised processing of personal data. Most of the time, lawmakers choose to use established privacy principles to support data protection regulations. In addition, most researchers

[375] Mor Bakhoum et al., 'Introducing a Holistic Approach to Personal Data' in Mor Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law, MPI Studies on Intellectual Property and Competition Law 28*, Germany, Springer-Verlag GmbH, 2018, 1-2.

[376] P. De Hert & S. Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in S. Gutwirth et al. (eds.), *Reinventing Data Protection?* Berlin, Springer, 2009, 3.

concurred that privacy and data protection have one thing in common: they are both subject to significant intrusion in the modern information society.[377]

Although the terms 'privacy' and 'personal data protection' are linked and frequently used interchangeably, they refer to two distinct concepts. In the EU, the concept of privacy is derived from ideas like human dignity and the rule of law. The terms 'privacy' and 'data protection' have different meanings in EU law, which distinguishes them as being related but distinct concepts that frequently overlap. While data protection refers to restrictions or requirements on the processing of data belonging to an identifiable individual, privacy often refers to the protection of a person's 'personal space.' On the other hand, data protection and privacy overlap in a way that makes data protection both broader and more specific than privacy, as noted by legal scholars. Data protection is more specific since it solely addresses the processing of personal data, whereas privacy covers a larger range of issues. However, data protection is also more comprehensive as it covers the processing of personal data, even if such data does not violate privacy.[378]

According to several definitions, privacy is a much broader notion that encompasses a variety of rights and values, including the right to be alone, personhood, familiarity, seclusion, and more other. Furthermore, data protection has a fundamental procedural nature that makes it more objective as a right in various circumstances, as opposed to privacy, whose illusive and subjective nature makes the right different in various contexts and countries. Finally, data protection serves other, additional fundamental rights and values in addition to privacy, making it more than just informational privacy in and of itself. The security of IS - known as 'data security' and the quality of the data they contain also known as 'data quality' are two interests that data protection regulations seek to protect in addition to privacy.[379]

There are substantial differences between privacy and data protection because the two are independent concepts with different scopes, purposes, and objectives. The fact that privacy and data protection cannot be substituted for one another is not only positivist; it has a deeper significance. Although protecting privacy undoubtedly takes centre stage in data protection law, it is inaccurate to suggest that protecting privacy is the only or even the

[377] Maria Tzanou, 'Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right' *International Data Privacy Law*, 2013, vol.3/2, 88-89.
[378] Politou et al., *Privacy and Data Protection Challenges in the Distributed Era*, 7.
[379] Tzanou, 'Data protection as a fundamental right next to privacy?', 88-89.

primary goal of this legislation. Data protection regulations serve a variety of interests, some of which go far beyond conventional notions of privacy. The provisions of data protection legislation rarely directly reflect intimacy-oriented views of privacy, and vice versa, larger privacy concepts are not suited to elucidate data protection tenets like purpose limitation. Last but not least, some scholars assume that recognising a separate right to data protection in addition to a right to privacy would show more respect for EU constitutional tradition.[380]

4.1.1. Regulation of privacy and data protection law at the EU level

In the past, the protection of privacy was usually considered by laws only from a narrow point of view, such as the confidentiality of correspondence and communications, the inviolability of the home, etc. A Sub-Committee of the European Committee on Legal Cooperation (CCJ) was tasked in 1971 with researching how contemporary scientific and technological advancements affect civil law components of the right to privacy. It concluded that priority should be given to protecting privacy concerning electronic data banks and discovered that Resolution No.3 held in Basel from May 15–18, 1972, on 'Protection of Privacy given the Increasing Compilation of Personal Data into Computers,' supported this position. To that purpose, on September 26, 1973, the Committee of Ministers adopted 'Resolution (73)22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector.'[381] The protection of the individual concerning electronic data banks has been a frequent topic of discussion by the Sub-Committee and, on 20 September 1974, 'Resolution (74)29 on, the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector was adopted.'[382]

The Parliamentary Assembly of the Council of Europe, taking into account the latest trend, recommended to the Committee of Ministers in its Recommendation 890 in 1980 to explore the possibility of including in the Human Rights Convention a provision on the

[380] De Hert & S. Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg', 9-10.
[381] Council of Europe Committee of Ministers, 'Resolution (73) 22 on The Protection of the Privacy of Individuals Vis-a-vis electronic data banks in the private sector' 26 September 1973 at the 224th meeting of the Ministers' Deputies), 1-9.
[382] Consultative Assembly, 'Committee on Science and Technology Sub-Committee, 'on'-Data Processing Resolution (74) 29 on the protection of the privacy of individuals vis-d-vis electronic data banks in the public sector, Strasbourg 13 November 1974, AS/Science/Computer (26) 2, 1-5.

protection of personal data. The need for such legal provisions arose given the increasing use of computers for administrative purposes. The result was the adoption of the Convention for the Protection of Individuals concerning Automatic Processing of Personal Data, which was opened for signature by the MS of the Council of Europe on 28 January 1981 at Strasbourg.[383] The purpose of the Convention was to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, concerning the automatic processing of personal data relating to him.[384] Additionally, several recommendations were adopted with topics ranging from medical databanks (1981) and police records (1987) to the protection of privacy on the internet (1999), profiling (2010), and social networking sites.[385]

It was evident that the Convention needed to be updated to better address new privacy challenges brought on by the increased use of new information and communication technologies, the globalisation of processing operations, and the ever-increasing flows of personal data. On May 18, 2018, the Committee of Ministers adopted the Protocol amending the Convention and approved the Explanatory Report as a component of the Protocol. The purpose of this Protocol was to modernise and strengthen the Convention (ETS No.108) and its Additional Protocol on supervisory authorities and transborder flows (ETS No.181).[386]

For the MS to protect the fundamental rights and freedoms of natural persons and in particular their right to privacy concerning the processing of personal data, the EU legislators have adopted Directive 95/46/EC on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (DPD) in 24 of October 1995.[387] The goal of the 1995 DPD was to harmonise data protection regulations across the EU to safeguard data subjects' fundamental rights and promote data exchange between the MS. The purpose of the EU data protection law became clear in that it was more connected

[383] Council of Europe, 'Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data', European Treaty Series - No. 108, Strasbourg, 28.I.1981, 1-16.
[384] Council of Europe, 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data', European Treaty Series - No. 108, Strasbourg, 28.I.1981, 1-9.
[385] Paul de Hert & Vagelis Papakonstantinou, 'The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition' *Computer Law & Security Review*, vol.30, 2014, 633-642.
[386] Council of Europe, 'Convention 108 +' Convention for the protection of individuals with regard to the processing of personal data, 2018, 5-16.
[387] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, 31–50.

with the protection of fundamental rights than with creating the EU market.[388] The DPD should not apply to the processing of personal data in the course of activities outside the scope of Community law, in particular in the case of processing of operations relating to public safety, defence, or national security, or by an individual in the course of purely personal or domestic activities. The DPD defined more precisely the conditions under which the processing of personal data is lawful (Art.5), the principles of data quality (Art. 6), and the criteria for making data processing legitimate (Art.7). The MS should prohibit the processing of special categories of data, especially personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. The person whose data is being processed, the data subject, has the right to obtain information (Art.10 and 11), the right of access to data (Art.12) and the right to object to the processing of data (Art.13). The DPD also clarified other aspects of data processing, such as exceptions and limitations to the rights of data subjects, confidentiality and security of data processing, notification of processing to the supervisory authority and the transfer of personal data to third countries.[389]

The DPD's main goal of removing obstacles to the free flow of personal data between the MS has been achieved, despite the implementation delays and gaps. Because of this, in its initial Report, the Commission hoped that this would assist governments, DPAs and operators in determining what needed to be done to improve the application of the Directive in the EU, with more zealous enforcement, better compliance, and greater awareness of data subjects and data controllers' rights and obligations.[390] According to the Commission, the DPD established a broad legal framework that was both technologically neutral and generally acceptable. For citizens, businesses, and authorities, the standardised set of regulations providing a high degree of protection for personal data throughout the EU has brought about significant benefits. The Commission at that time believed that the DPD formed a general legal framework that met its original goals because there was an expectation of successful ratification of the Constitutional Treaty, which would later have a significant impact on the

[388] Gabriela Zanfir, 'Tracing the Right to Be Forgotten in the Short History of Data Protection Law: The "New Clothes" of an Old Right' in S. Gutwirth et al. (eds.), *Reforming European Data Protection Law, Law, Governance and Technology Series 20,* Dordrecht, Springer, 2015, 227-249.
[389] Directive 95/46/EC, OJ L 281, 23.11.1995, 31–50.
[390] Commission of The European Communities, 'Report from the Commission First report on the implementation of the Data Protection Directive (95/46/EC)', Brussels, 15.5.2003 COM (2003) 265 final, 27.

right to the protection of personal data. As a result, the Commission did not intend to submit any legislative proposal to amend the DPD.[391]

Likewise, the establishment of the WP29 by the passage of the DPD further entrenched the function of data privacy authorities in local politics. The WP, which was made up of national data privacy authorities, formally enlisted the network of MS regulators in the process of developing and implementing supranational regulations. The WP has been instrumental in the externalisation of EU data privacy policy since its creation and acted as a cutting-edge example of how to structure transnational governance.[392]

To protect the fundamental rights and liberties of natural persons and the legitimate interests of legal persons in the case of public communications networks, specific legal, regulatory, and technical provisions should be made, especially in light of the growing capacity for automated storage and processing of subscriber and user data. As the result, Directive 2002/58/EC on privacy and electronic communications or shortly 'e-PD' was enacted on July 12, 2002. This Directive provided for the harmonisation of national provisions necessary to ensure an equivalent level of protection of fundamental rights and freedoms, in particular, the right to privacy and confidentiality, concerning the processing of personal data in the e-communications sector, as well as to ensure the free movement of such data and e-communications equipment and services in the Community.[393]

Even though the e-PD was updated in 2009 to provide clearer rules on governing online communications, it required additional updating to ensure that it was ready for the difficulties of the new digital age. One of the primary measures aimed at bolstering trust and security in digital services in the EU was the continuing revision of this legislation. The applicability of existing laws, citizens' perspectives on potential modifications to e-privacy regulations, and their views on online privacy were all of interest to the European Commission.[394]

The e-PD's rules were put to the test in 2015 when the Commission determined it was necessary to examine whether these rules had achieved their primary goals of ensuring the

[391] Commission of The European Communities, 'Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive', /COM/2007/0087 final, 9.
[392] Abraham L. Newman, *Protectors of Privacy: Regulating Personal Data in the Global Economy,* Ithaca, Cornell University Press, 2008, 75-76.
[393] Directive 2002/58/EC on privacy and electronic communications, OJ L 201, 31.7.2002, 37-47.
[394] European Commission, 'Flash Eurobarometer 443: Briefing note e-Privacy', 2016, 1.

privacy and confidentiality of communications within the EU and whether these rules were still appropriate given the regulatory and technological environment. According to the Better Regulation guidelines, the e-PD was evaluated for Regulatory Fitness and Performance (REFIT18) based on a range of characteristics. The e-PD's provisions were still fully applicable to achieve the goals of protecting communication privacy and confidentiality, although certain of its provisions were no longer appropriate in light of changes in the legal environment, market trends, and technology. Overall, the e-PD seemed to have given an adequate foundation for safeguarding the privacy and confidentiality of communications in the EU; but several problems were found with its efficacy. The study also demonstrated that an adequate system for monitoring the application of the e-PD was presently lacking and should be put in place in the future, based on the fact that the quantitative evidence was still scant.[395]

The goal of the DSM Strategy[396] was to improve the security and trust of digital services. A crucial step toward achieving this was the revision of the data protection framework, specifically the adoption of GDPR (EU) 2016/679.[397] To provide e-communications service users with a high degree of privacy protection and to create a level playing field for all market participants, the DSM Strategy also examined the e-PD, guaranteeing compliance with the GDPR and anticipating goals for the DSM Strategy. Insofar as e-communications data that qualify as personal data was concerned, this proposal was '*lex specialis'* to the GDPR and would particularise and complement it. There were no particular requirements for data retention in that proposal. It was also suggested that legal persons associated with legitimate interests in communications should be protected. By preventing differing interpretations in the MS, the Commission presented a proposal for a Regulation to ensure consistency with the GDPR and legal clarity for both users and companies. Regulation

[395] European Commission, 'Commission Staff Working Document Impact Assessment Accompanying the document Proposal for Regulation of The European Parliament and Of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)', Brussels, 10.1.2017, SWD (2017) 3 final, Part 2/3, 6-8.
[396] European Commission, 'Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions A Digital Single Market Strategy for Europe', Brussels, 6.5.2015 COM (2015) 192 final, 8.
[397] Regulation (EU) 2016/679, OJL 119, 1–88.

could provide an equal level of protection for users across the EU and reduce compliance costs for companies that operated internationally.[398]

The outcome of the public consultation on the evaluation and review of the e-PD showed that the e-PD had not achieved, or has only partially achieved, the goal of ensuring complete protection of privacy and confidentiality of communications throughout the EU. The majority of challenges, according to reports from citizens, consumers, and civil society organisations, were related to applying and comprehending the rules. The initial rules concerned unsolicited commercial communications that were imprecise in their application to non-electronic communication services, unclear in their mix of an opt-in and opt-out system, and as the result, the '*spam'* continued to happen. The next was the confidentiality of e-communications, which excluded over-the-top services, and was viewed with suspicion. Since there were many competent authorities, the e-PD and GDPR did not align, therefore the final rules concerned the notification of data breaches. As a result, important clauses might have been applied differently by MS. The e-PD left it up to the MS to name a competent authority or other national entities, whereas then the DPD, now the GDPR entrusted its implementation to data protection supervisory authorities. This has led to a situation that has become fragmented.[399]

In January 2017, the Commission published a proposal for a regulation that would replace the e-PD and would deal with the protection of personal data in e-communications. The reform aimed to bring the laws governing e-communications into compliance with the GDPR-enacted data protection regime. All individuals, telecom operators and enterprises would benefit from the same degree of protection for their e-communications under the new regulation, which would be directly applicable throughout the EU. The new participants offering e-communications services that were not covered by the e-PD would also be subject to the proposed rules on the confidentiality of e-communications.[400]

---

[398] European Commission, 'Proposal for a Regulation of The European Parliament and Of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' Brussels, 10.1.2017, COM (2017) 10 final, 2017/0003 (COD), 2.

[399] European Commission, 'Synopsis Report of The Public Consultation on The Evaluation and Review of the e-Privacy Directive', 2016, 2-3.

[400] European Union Agency for Fundamental Rights and Council of Europe, 'Handbook on European data protection law 2018 edition', Publications Office of the European Union, Luxembourg, 2018, 34.

The content of e-communications might contain extremely private information about the involved end-users. Likewise, the CJEU acknowledged that metadata obtained from e-communications might sometimes expose extremely sensitive and personal information. The vast majority of MS also acknowledged the necessity for e-communications to be protected as a separate fundamental right. Last but not least, to preserve compliance with the GDPR, it was required to examine the e-PD and take action to harmonise these two documents. The e-PD's implementation has not been successful in empowering the end-users. To accomplish the goal, the concept must be put into practice by centralising consent in software and providing users with information about the privacy settings within. The supervisory authorities and the GDPR's consistency mechanism are how this Regulation would be enforced.[401] Since the proposed legislation has not yet been able to achieve consensus among MS of EU, negotiations on E-Privacy Regulation (e-PR) are still ongoing. It is most definitely not anticipated that the e-PR would go into effect until 2023. Any new restrictions would not go into force until 2025 after a likely 24-month transitional period.[402]

4.1.2. Summary

As is apparent from the technological development and Internet maturation of society, digital transformation affects all users and business organisations. However, as users rely on these organisations on the Internet and share their credentials with them, their privacy and privacy rights are violated much more. Therefore, to gain their trust and increase their confidentiality, the data protection law guarantees users the rights and control over the processing of their data. At the same time, the data protection law also holds the organisations responsible for their non-compliance approaches, which are contrary to what they intend to require. While the right to privacy, being a substantive right, is one of the fundamental human rights and is related to personal space, the right to data protection, being a procedural right, covers the stages of processing data belonging to an identifiable person. However, it cannot be overlooked that these two rights are being affected by new advanced technologies and are raising one of the most debated user concerns from the EU perspective.

[401] European Commission, 'Proposal for a Regulation' COM (2017) 10 final, 2017/0003 (COD), 2-5.
[402] Florian Dietrich & Dr. Reemt Matthiesen, CMS: e-Privacy European Regulation on Privacy and Electronic Communications, <https://cms.law/en/deu/insight/e-privacy> accessed 20 Aug. 2023.

4.2. GDPR as the next-generation data protection law

Globalisation and rapidly advancing technology have created new difficulties for the protection of personal data. Personal data is now being collected and shared on a far larger basis. The utilisation of personal data for business and government purposes is now possible on a never-before-seen scale due to technology. Personal information is being made more widely and publicly available by natural individuals. Technology has revolutionised both business and social life, and it should make it easier for personal data to be transferred freely inside the Union as well as to other nations and international organisations while yet maintaining a high level of privacy protection. Given the significance of building the trust that would allow the digital economy to flourish across the internal market, those trends call for a strong and more unified data protection framework in the Union, supported by effective enforcement. Natural individuals ought to be in charge of personal data.[403]

In light of this, the Commission determined in its Communication of November 4, 2010, that while the goals and underlying principles of the DPD remain relevant, the world has changed dramatically as a result of rapid technological advances and new personal data security challenges. As a next step, the Commission put forth legislation in 2011 intending to update the legal framework for data protection to strengthen the EU's position on protecting the individual's personal data in the context of all EU policies, including law enforcement and crime prevention while taking into account these sectors' unique characteristics.[404]

By resolution dated July 6, 2011, the European Parliament accepted a Report that backed the Commission's strategy for updating the data protection framework. On February 24, 2011, the Council of the EU approved conclusions in which it broadly endorsed the Commission's desire to alter the data protection framework and concurred with many aspects of its strategy. The proposal was based on Art.16 TFEU, the new legal groundwork provided by the Lisbon Treaty enabling the introduction of new data protection laws. This clause permits the adoption of regulations about the protection of people while the MS process

[403] Regulation (EU) 2016/679, OJL 119, 1–88.
[404] European Commission, 'Communication from The Commission to The European Parliament, The Council, The Economic and Social Committee and The Committee of The Regions: A comprehensive approach on personal data protection in the European Union', Brussels, 4.11.2010 COM (2010) 609 final, 1-20.

personal data when engaging in activities covered by the EU law. Additionally, it permits the implementation of regulations governing the free flow of personal data, including that handled by the MS or commercial entities. The best legal instrument for defining the framework for the protection of personal data in the Union is thought to be a regulation. By establishing a unified set of fundamental rules, enhancing the protection of individuals' fundamental rights, and supporting the operation of the Internal Market, the direct applicability of a Regulation following Art.288 TFEU would lessen legal ambiguity and increase legal certainty. As the result, a proposal for a Regulation on the protection of individuals concerning the processing of personal data and on the free movement of such data was presented by the European Commission on January 25, 2012.[405] Later, on April 27, 2016, the European Parliament and the Council adopted GDPR (EU) 2016/679, which repealed Directive 95/46/EC, with the effect of applying from 25 May 2018.[406]

To ensure the fundamental right to the protection of personal data, strict data protection laws are required. They play a crucial role in democratic societies and are crucial to the development of a data-driven economy. The EU seeks to address both the challenges posed by digital transformation and the numerous opportunities it presents in terms of services, employment, and innovation. The GDPR is in effect throughout the EU as of 2018. In addition to this, the Data Protection Law Enforcement Directive[407] and the Data Protection Regulation for EU institutions and bodies[408], are at the centre of a consistent and well-organized EU data protection agenda. The e-Privacy Regulation, which is now undergoing legislative action, would complete this framework.[409]

---

[405] European Commission, ''Proposal for A Regulation of The European Parliament and Of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012 COM (2012) 11 final 2012/0011 (COD), 2.

[406] Regulation (EU) 2016/679, OJL 119, Art. 99.

[407] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJL 119, 4.5.2016, 89-131.

[408] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, PE/31/2018/REV/1, OJ L 295, 21.11.2018, 39-98.

[409] European Commission, 'Communication from The Commission to The European Parliament and The Council Data protection rules as a trust-enabler in the EU and beyond – taking stock', Brussels, 24.7.2019, COM (2019) 374 final, 1.

4.2.1. General provisions of the GDPR

In its GDPR proposal, the European Commission identified three key areas for assessment and considered why the time has come for a stronger data protection system in the EU. Legal uncertainty and public opinion about the risks associated with online activities were common, as the existing legal framework did not prevent the fragmentation of personal data protection measures that were applied throughout the Union. The main initial topic was to allow the digital economy to develop in the domestic market, supported by strong enforcement. The next problematic area has to do with allowing individuals to control their personal data. The final challenge was to strengthen legal and practical certainty for economic operators and public authorities.[410]

In addition, as technology can advance the cause of data protection, technical advancement might potentially profit from improved data protection implementation and efficacy. It is important to note two concepts in this regard. The first concept is the reciprocity of benefits. It means that in the same way that data controllers can use technological applications to make it easier to handle data for their purposes, data subjects should be able to use those same technologies to exercise their rights. The most notable of them is the right to withdraw consent and other access and informational rights. From the clauses referring to 'privacy by design' or 'privacy by default,' a second strategy can be inferred. The GDPR seeks to address the difficulty of integrating data protection with technology to ensure adherence to legal requirements.[411]

The GDPR, in particular, aims to 'Europeanise' data protection law and make it more effective with the introduction of a regulation rather than a directive, an effort is made to minimise national differences while also establishing important new channels for private redress and governmental enforcement. Although National Supervisory Authorities (NSAs) are primarily in charge of public enforcement of the framework, the establishment of a new

[410] European Commission, 'Proposal for A Regulation of The European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)', Brussels, 25.1.2012 COM (2012) 11 final 2012/0011 (COD), 2

[411] Yves Poullet, 'Is the general data protection regulation the solution?' *Computer law & Security review*, vol.34, 2018, 773-778.

EU body with the power to issue authoritative opinions and, in certain circumstances, binding decisions has a centralising effect on data protection enforcement. The modifications brought about by the GDPR are anticipated to improve the effectiveness of the EU Charter's rights to privacy and data protection in the long run. The GDPR places more responsibility on national legislatures, the NSAs and the courts, despite this shift towards a true EU legal framework for data protection.[412]

In general, it is believed that the growing technological capacity for data collection and processing poses a serious risk to individual privacy. As a result, data protection law helps to protect privacy to the extent that it serves as a control on excessive authority over personal information. In this regard, one could claim that the GDPR serves as a tool to secure the security of personal information and more. In conclusion, since the GDPR is an important tool to prevent the erosion of privacy in the digital age, it contains a list of requirements that must be met to maintain privacy in the processing of data.[413]

The GDPR sets out rules regarding the protection of individuals through the processing of personal data and rules regarding the free movement of personal data. The GDPR protects the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. The free movement of personal data within the Union is not restricted or prohibited for reasons related to the protection of individuals in the processing of personal data. The processing of personal data must be designed to serve humanity. The right to the protection of personal data is not absolute; it must be regarded with its function in society and balanced against other fundamental rights under the principle of proportionality.[414]

Art.2 determines the GDPR's material scope which applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.[415] It can be assumed that Art.2 encompasses both the public and private sectors

[412] Jorrit J. Rijpma (Ed.), *The New Eu Data Protection Regime: Setting Global Standards for The Right to Personal Data Protection*, The XXIX Fide Congress in The Hague 2020 Congress Publications, Eleven International Publishing, The Hague, 2020, vol.2, 1.
[413] Jef Ausloos, *The Right to Erasure in EU Data Protection Law from Individual Rights to Effective Protection,* Oxford University Press, Oxford, 2020, 77.
[414] Regulation (EU) 2016/679, OJL 119, Rec.4.
[415] Ibid, Art.2.

since it makes no distinction between the two. However, the second paragraph excludes some processing operations from the GDPR's scope, such as the processing of data for purely personal or household activities.[416] Art.3 of the GDPR defines the territorial scope of data processing in the context of the activities of an 'establishment' of a controller or processor in the Union (*Google Spain* (C-131/120), regardless of whether the processing takes place in the Union or not. The second part of Art.3 affects the processing of personal data of data subjects who are in the Union by a controller or processor not established (*Weltimmo* (C-230/140) in the Union, where the processing activities are related to certain circumstances. The last part of Art.3(3) involves the processing of personal data under specific situations in a place where MS law applies under public international law.[417] As can be seen from the provisions of the Article, the territorial scope is one of the main defining aspects for both data controllers (processors) and data subjects, since if they do not meet this criterion, the GDPR will not apply.

Art.4 (1) defines that 'personal data' means *any information relating to an identified or identifiable natural person* ('data subject') and 'an identifiable natural person' is who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Data protection principles should apply to any information relating to an identified or identifiable natural person. Personal data which have experienced pseudonymization, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. 'Pseudonymization' is the processing of personal data in a way that prevents the personal data from being associated with a specific data subject without the use of additional information, provided that the additional information is kept separately and is subject to technical and organisational measures to ensure that personal data does not relate to an identified or identifiable natural person.[418]

[416] Herke Kranenborg 'Article 2. Material scope' in Christopher Kuner, Lee A. Bygrave & Xe Christopher Docksey *The EU General Data Protection Regulation (GDPR): A Commentary,* New York, Oxford University Press, 2020, 63.
[417] Regulation (EU) 2016/679, OJL 119, Art.30.
[418] Ibid, Art.4.

There is also non-personal data that does not fall within the GDPR's definition of personal data. The non-personal data can be divided into data that did not initially relate to a named or identifiable natural person and information that was once personal but now has been made anonymous. The 'anonymization' of personal data differs from pseudonymisation in that properly anonymized data are non-personal data because they cannot be associated with a specific individual, not even with the aid of additional information.[419]

The Working Paper states that the concept of personal data has four key structural components, which were later incorporated into the GDPR's interpretation. The initial meaning of 'any information' has a broad meaning of personal data. According to the nature of the information, any statements about a person are considered to be personal data. Information need not be accurate or backed up by evidence to qualify as 'personal data.'[420] This element was used by CJEU in the *Nowak* case (C-434/16) judgment by mentioning that '[T]he use of the expression 'any information' in the definition of the concept of 'personal data', reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject.'[421]

The second component is the definition of 'related to,' which is essential since it is critical to determine precisely which relationships or ties are relevant and how to tell them apart. In general, when information is about a specific person, it can be said to 'relate' to that person.[422] In *Nowak's* case (C-434/16) the CJEU noted 'that 'relates' to the data subject, it is satisfied where the information, because of its content, purpose or effect, is linked to a particular person.'[423] The 'identified or identifiable' natural person is the third component. A natural person is often seen as being 'identified' when, within a group of people, he or she is 'distinguished' from all other group members.[424] A natural person's ability to be directly or

[419] European Commission, 'Communication from The Commission to The European Parliament and The Council Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union', Brussels, 29.5.2019 COM (2019) 250 final, 5-6.
[420] Article 29 Data Protection Working Party (DPWP), 'Opinion 4/2007 on the concept of personal data', 01248/07/EN, WP 136, Adopted on 20th June, 6-7.
[421] *Peter Nowak v Data Protection Commissioner,* Judgment of the Court (Second Chamber) of 20 December 2017, Case C-434/16, 20.12.2017, para.34.
[422] Article 29 DPWP, 'Opinion 4/2007 on the concept of personal data', 9-11.
[423] *Peter Nowak v Data Protection Commissioner*, Case C-434/16, para. 35.
[424] Article 29 DPWP, 'Opinion 4/2007 on the concept of personal data', 12-14.

indirectly identified by the controller or another person should be taken into consideration when determining whether that natural person is identifiable.[425] In *Breyer* (Case C-582/14), case CJEU stated that 'it is not required that all the information enabling the identification of the data subject must be in the hands of one person.'[426]

The last component is the 'natural person' which is a human being.[427] No matter their nationality or place of residence, natural persons are covered by the protection provided by GDPR when it comes to the processing of their personal data. The processing of personal data related to legal persons, specifically undertakings constituted as legal persons, including the name, form, and contact information of the legal person is not covered by GDPR.[428] However, in a variety of situations, certain data protection rules may still indirectly apply to information on corporations or legal persons.[429] Just like in *Schecke and Eifert* cases (C-92/09 and C-93/09) the CJEU stated 'legal persons can claim the protection of Articles 7 and 8 of the EU Charter concerning such identification only in so far as the official title of the legal person identifies one or more natural persons.'[430]

Setting data processing to personal data and pseudonymous data, but excluding anonymous data from its scope, would also have some consequences. Because anonymous data is everywhere these days, from e-commerce websites to big data apps. As the data has been anonymous, the data subject cannot be identified, and the anonymous data is not linked to any identified or identifiable natural person or personal data. Therefore, the GDPR will not apply to the data subject if they anonymized their personal data out of concern for their privacy. However, the data subject will unquestionably fall within the GDPR rule if they provide information that is personal or pseudonymous data. Due to the lack of a clear understanding of how anonymization works in practice, this resulting stance puts data subjects in a difficult decision regarding whether or not to disclose or anonymize the data.

4.2.2. The principles and conditions in consent of the processing of the data

[425] Regulation (EU) 2016/679, OJL 119, Art. 4.
[426] *Patrick Breyer v Bundesrepublik Deutschland,* Judgment of the Court (Second Chamber) 19 October 2016, Case C-582/14, para.43-46.
[427] Article 29 DPWP, 'Opinion 4/2007 on the concept of personal data, 12-14.
[428] Regulation (EU) 2016/679, OJL 119, Rec.14.
[429] Article 29 DPWP, 'Opinion 4/2007 on the concept of personal data, 12-14.
[430] *Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen,* Judgment of the Court (Grand Chamber) 9 November 2010, Joined cases C-92/09 and C-93/09, para. 53.

Following Art.5 of the GDPR, the key principles for the processing of personal data are a) lawfulness, fairness and transparency; b) purpose limitation; c) data minimization; d) accuracy; e) storage limitation; f) integrity and confidentiality and g) accountability. One of the main principles relating to the processing of personal data is '*lawfulness, fairness and transparency*' which means that personal data should be processed lawfully, fairly and transparently concerning the data subject.[431] Compared to other rules governing the data protection area, the core principles of data protection have not undergone any significant changes for several decades.[432] According to GDPR, 'processing' means any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Nevertheless, processing of personal data should be lawful only if at least one of the following applies which are a) the consent given by the data subject; b) for the performance of a contract; c) for compliance with a legal obligation; d) to protect the vital interests of the data subject; e) for the performance of a task carried out in the public interest or f) for purposes of the legitimate interests pursued by the controller or by a third party.[433]

The 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.[434] The GDPR's Art.6 lists six legal justifications for processing personal data, with consent remaining one of them. A data controller must always take the time to examine what would be the proper legal basis for the anticipated processing before starting any activities that include processing personal data.[435]

---

[431] Regulation (EU) 2016/679, OJL 119, Art. 5.
[432] Cecile De Terwangne 'Article 5. Principles relating to processing of personal data' in Christopher Kuner, Lee A. Bygrave & Xe Christopher Docksey *The EU General Data Protection Regulation (GDPR): A Commentary*, New York, Oxford University Press, 2020, 311.
[433] Regulation (EU) 2016/679, OJL 119, Art. 6.
[434] Ibid, Art. 4.
[435] Article 29 DPWP, 'Guidelines on consent under Regulation 2016/679', Adopted on 28 November 2017 as last Revised and Adopted on 10 April 2018, 17/EN WP259 rev.01, 3.

Four essential requirements are valid for data subject consent which can be inferred from the provisions of Art.4(11) GDPR: the consent must be a) freely given, b) specific, c) informed, and d) unambiguous. The fact that these requirements add up to a high threshold for legitimate consent. The tendency of the DPAs to closely interpret each criterion also contributes to this high barrier.[436] The word 'free' indicates that data subjects have genuine autonomy and choice. The GDPR states that consent is generally not legitimate if the data subject has no real choice, feels obliged to consent, or will suffer penalties if they do not consent. The requirement of the consent to be 'specific' attempts to provide the data subject with some level of user control and transparency. The GDPR has not altered this need, which is still closely related to the need for 'informed' consent. Regardless of the rules governing the compatibility of objectives, consent must be tailored to the goal. With the knowledge that they are in charge and that their data will only be used for those purposes, data subjects will grant their consent. If a controller uses consent to process data and then wants to use it for another purpose, the controller must obtain further consent for that purpose unless there is another legal basis that more accurately represents the circumstances. The GDPR strengthens the requirement that informed consent be given. The necessity for transparency is one of the core aspects, closely related to the ideals of fairness and lawfulness, according to Art.5 of the GDPR. For data subjects to make informed decisions, comprehend what they are agreeing to, and exercise their right to withdraw their consent, information must be provided to them before getting their consent. If the controller does not make information easily accessible, the user control is rendered useless and consent is rendered ineffective as a legal foundation for processing. If the conditions for informed consent are not met, the result will be that the consent will be void and the controller may be in violation of Art.6 of the GDPR.[437]

The data subject's consent to the processing of their personal data should be expressed in a clear, affirmative act that is freely given, specific, informed, and unambiguous, such as a written statement, including one made electronically, or an oral statement. This could involve making a clear indication that the data subject agrees to the proposed processing of his or her personal data, such as by ticking a box when accessing an internet website or selecting

[436] Lee A. Bygrave & Luca Tosani 'Article 4(11). Consent' in Christopher Kuner, Lee A. Bygrave and Xe Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary*, New York, Oxford University Press, 2020, 181.
[437] Article 29 DPWP, 'Guidelines on consent under Regulation 2016/679', 5-16.

technical options for information society services. Therefore, silence, pre-ticked boxes, or silence should not be interpreted as consent. All processing carried out for the same purpose or purposes should be covered by consent. Consent must be provided for each of the processing's numerous purposes. When processing is enabled by the data subject's consent, the controller must be able to demonstrate that the data subject has given consent for the processing of his or her personal information. If the consent of the data subject is provided as part of a written declaration that also addresses other issues, the request for consent must be presented in a way that makes it apparent that it is distinct from the other issues, in an understandable and accessible format, and a plain language. Any portion of such a declaration that violates this Regulation shall not be enforceable. In contrast to the DPD, which did not specifically mention consent withdrawal, the GDPR stipulates that the data subject has the right to withdraw consent at any time. The lawfulness of processing based on consent before its withdrawal shall not be impacted by the withdrawal of consent. The data subject must be informed before providing consent. Both giving and withdrawing consent must be simple processes.[438]

The EU regulators have underlined the deficiencies in the previous system and the lack of individual control over personal data. The newly passed GDPR was anticipated to have revolutionary effects, however, this was not the case. Although the list of rights of data subjects has been expanded in the newly adopted GDPR, their legal status has not changed significantly. The 1995 DPD's legacy is heavily incorporated into the list of data subject rights, however, the GDPR did include several innovative approaches to modernise the control rights framework. An examination of the GDPR reveals that many of its provisions were taken directly from the law, including consumer protection law, property law, and competition law. Along these lines, the GDPR seems to imply that the EU data protection law may have hope at the end of the tunnel if it can be understood holistically. The rules regarding data portability, the right to be forgotten, and the right to information are some of the most notable examples of introducing solutions from other legal disciplines.[439]

[438] Regulation (EU) 2016/679, OJL 119, Art. 7.

[439] Helena Ursic, 'The Failure of Control Rights in the Big Data Era: Does a Holistic Approach Offer a Solution?' in Mor Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law, MPI Studies on Intellectual Property and Competition Law 28,* Germany, Springer-Verlag GmbH part of Springer Nature 2018, 57-58.

4.2.3. The rights of the data subjects

The purpose of Art.12 of the GDPR is to ensure that information and access rights are effectively exercised, mainly for the benefit of data subjects and secondarily for the benefit of data controllers. There are technical and procedural rules surrounding the exchange of information between data controllers and data subjects, but no substantive rights are defined or established. The fundamental premise of this article is that the substantive rights of data subjects can only be supported through transparent, reasonable, and efficient methods. In this regard, Art.12 specifies the circumstances under which data subjects must be kept informed of the processing of their personal data, either actively or passively.[440]

The controller must take the necessary steps to ensure that the data subject receives any information referred to in Articles 13 and 14 as well as communications under Articles 15 to 22 and 34 regarding processing in a clear, transparent, understandable, and easily accessible format. This is especially true for any information targeted directly at children. The information should be delivered in writing or by other methods, including electronic ones when appropriate. If the subject requests it, the information may be given verbally as long as the subject's identification can be established in some other way. The controller must make it easier for data subjects to exercise their rights as described in Articles 15 to 22. Unless the controller can prove that it is unable to identify the data subject, he/she should not refuse to act on the data subject's request to exercise his or her rights under Articles 15 to 22 in the situations mentioned in Art.11(2).[441]

The effectiveness of legal rules in general, and data subjects' rights in particular, depends to a considerable extent on the existence of appropriate mechanisms to enforce them. In the digital age, data processing has become ubiquitous and increasingly difficult for individuals to understand. To mitigate power imbalances between data subjects and

[440] Radim Polcak 'Article 12. Transparent information, communication and modalities for the exercise of the rights of the data subject' in Christopher Kuner, Lee A. Bygrave and Xe Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary,* New York, Oxford University Press, 2020, 401.
[441] Regulation (EU) 2016/679, OJL 119, Art. 12.

controllers, individuals have been given certain rights to exercise greater control over the processing of their personal information.[442]

The controller must inform the data subject without undue delay and, in any case, within one month of receiving the request about any actions taken in response to a request made following Articles 15 to 22. Depending on the difficulty and volume of the requests, that time frame may be extended by an additional two months. Within one month of receiving the request, the controller must notify the data subject of any such extension and justify the delay. Whenever possible, information should be delivered electronically when the data subject submits a request through an electronic form, unless the data subject specifically requests otherwise. If the controller declines to act on the data subject's request, the controller must promptly notify the data subject - at the latest within one month of receiving the request - with the reasons why, as well as the possibility of filing a complaint with a supervisory authority and pursuing a legal remedy. All communications and measures done following Articles 15 to 22 and 34, as well as the information given under Articles 13 and 14, should be free of charge. When a data subject makes requests that are unreasonable or excessive, especially given their recurrent nature, the controller may: a) levy a reasonable fee that takes into consideration the administrative expenses incurred in providing the requested information, communication, or action; or b) decline to comply with the request. It is the controller's responsibility to show that the request is extreme or unjustified.[443]

Under Art. 13-14 of GDPR, if the personal data of a data subject is collected from the data subject or not from the data subject, the controller should provide the data subject with all of the following information at the time the personal data is collected: a) the controller's name and, if relevant, the controller's representative's contact information; b) the data protection officer's contact information, if relevant; c) the intended uses for the processing of the personal data as well as the legal justification for the processing; d) when Article 6(1), point (f), is the basis for the processing, the controller's or a third party's legitimate interests are being pursued; e) the recipients of the personal data or groups of recipients, if any or f) if necessary, information about the controller's plans to transfer personal data to a third country

[442] European Union Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law 2018 edition', 205.
[443] Regulation (EU) 2016/679, OJL 119, Art. 12.

or international organisation, as well as the existence or lack of a Commission adequacy finding.[444]

The GDPR outlines the rights that data subjects have over their personal data, and when those rights are properly exercised, they are given a greater understanding of and control over their personal data. Organisations are required under the GDPR to be transparent about how they process data and to give people back control over their personal information. It establishes deadlines for organisations to respond to subject access requests and adds additional rights, like the right to data portability, that take care of some unresolved problems that have emerged since the DPD's creation. Understanding these expanded or new rights completely and identifying the methods and procedures that will need to be implemented or changed to comply with the GDPR are the main concerns from an organisational standpoint.[445]

The GDPR defines 2 main actors in data processing activities relating to personal data, the rights of data subjects and the obligations of data controllers. The data subject is an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The 'controller' means the natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data. The third important participant is the 'processor' which means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.[446]

In general, the processing of a data subject's personal information by data controllers is governed by Articles 12 through 14 of the GDPR, which gives transparency, modalities, information, and access measures. Articles 15-22 of the GDPR require that data controllers grant data subjects several rights related to the processing of personal data, namely the right of access (Art.15), the right to rectification (Art.16), the right to erasure (the right to be forgotten) (Art.17), the right to restriction of processing (Arts.18-19), the right to data

[444] Ibid, Art. 13-14.
[445] IT Governance Privacy Team, 'EU General Data Protection Regulation (GDPR) An implementation and compliance guide', UK, IT Governance Publishing Ltd, 2020, 63.
[446] Regulation (EU) 2016/679, OJL 119, Art. 4.

portability (Art.20), the right to object (Art.21) and the right not to be subject to a decision based solely on automated processing, including profiling (Art.22).

4.2.3.1. Right of access by the data subject

As the first step of the right of access, the data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed. Later, if the processing of personal data takes place, the data subject has access to the personal data and the following information a) the purposes of the processing; b) the categories of personal data concerned; c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period. And the last step, the controller must provide a copy of the personal data being processed. For any additional copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. If the data subject makes a request by electronic means, and unless the data subject requests otherwise, the information must be provided in a commonly used electronic form.[447]

The data subject should have the right to access the personal data that has been collected about him or her and exercise this right easily and at reasonable intervals to know and verify the lawfulness of the processing. This includes the right of data subjects to access data relating to their health, such as data in their medical records containing information such as diagnoses, test results, physician evaluations, and any treatment or intervention provided. Therefore, each data subject should have the right to know and obtain communication, in particular concerning the purposes for which personal data are processed, if possible, the period of processing of personal data, the recipients of personal data, the logic involved in any automatic processing of personal data and, at least based on profiling, the consequences of such processing. The controller should, whenever possible, be able to provide the data subject remote access to a secure system that would give him or her immediate access to their personal information. This right should not impair the freedoms or rights of others, particularly their

[447] Ibid, Art.15.

ability to safeguard their trade secrets, intellectual property, or software under copyright. But the outcome of those circumstances should not be a rejection to give the data subject all the information. Where a controller processes a large amount of information about a data subject, the controller should be able to request that, before providing the information, the data subject indicate the information or processing activities to which the request relates.[448]

The data subject's right to access serves two purposes in particular: it increases transparency and makes management easier. It improves transparency by giving the data subject access to a second, deeper, and more in-depth layer of information beyond what the controller discloses in the data protection notices provided following Articles 13 or 14 of GDPR. At any time following the moment of collection, and in theory without charge, it enables the data subject to request copies of the personal data being processed as well as updated information compared to what was stated in the notification. Since the GDPR does not regulate representation concerning access requests, any legal representation is governed by MS law, for example, via power of attorney. Nonetheless, a third party could assist the data subject in submitting a request to the controller. In terms of processing children's personal data, the GDPR is silent on who should make an access request. The rule that the right of access belongs entirely to the data subject is fully applicable. As a result, it should be permissible for minors to make valid access requests. This is especially true when children consent to the use of their personal data.[449]

There are several CJEU decisions regarding the interpretation of the right to access one's personal data based on the existing data protection regulation. In the *Rijkeboer case* (C-553/07), Mr. Rijkeboer requested the controller (the college) to notify him of all instances in which data relating to him from the local authority personal records had, in the two years preceding the request, been disclosed to third parties. He wished to know the identity of those persons and the content of the data disclosed to them. His first concern was that personal data kept by the local authority about a person, such as his name and address, which in the present case constituted 'the basic data.' It is apparent from the oral observations submitted by the controller that those data may be stored for a long time. Those basic data here constituted

[448] Ibid, Rec.63.
[449] Gabriela Zanfir-Fortuna 'Article 15. Right of access by the data subject' in Christopher Kuner, Lee A. Bygrave and Xe Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary*, New York, Oxford University Press, 2020, 452-461.

'personal data' within the meaning of Art.2(a) of the DPD since they represent information relating to an identified or identifiable natural person. Emphasising the importance of protecting privacy, the Court found that the right to privacy means that the data subject can be sure that his personal data is processed correctly and lawfully, that is, in particular, that basic data about him is accurate and disclosed to authorised recipients. As stated in Rec.l41 of the preamble to the DPD, to carry out the necessary checks, the data subject must have the right of access to the data relating to him that is being processed. The Court also affirmed that, in the present case, rules limiting the storage of information on the recipients or categories of recipients of personal data and on the content of the data disclosed over one year and correspondingly limiting access to that information, while basic data is stored for a much longer period, do not constitute a fair balance of the interest and obligation at issue, unless it can be shown that longer storage of that information would constitute an excessive burden on the controller. Ultimately, the Court held that Art.12 of DPD requires the MS to ensure a right of access to information on the recipients or categories of recipient of personal data and the content of the data disclosed not only in respect of the present but also in respect of the past. And it is up to the MS to set the retention period for this information and ensure access to this information.[450]

In *YS's case*, YS, a third-country national who applied for a residence permit for a fixed period in the Netherlands, requested to get access to 'the minute' relating to the decision of his application for a residence permit for a fixed period under asylum law. Nevertheless, YS's request was refused. However, the decision did give a summary of the data contained in the minute, the origin of those data and the bodies to which the data had been disclosed. YS objected to the refusal to communicate the minute, which itself was rejected by the decision. The Court had to decide whether there is a right to a copy of documents in which personal data have been processed, or whether the words 'right of access' could be interpreted to mean that there is a right to a copy of documents in which personal data have been processed, and also whether a legal analysis, as set out in a 'minute', be regarded as personal data? The Court agreed that the answer to the first and second questions is that the DPD must be interpreted as meaning that the data relating to the applicant for a residence permit contained in the minute

[450] *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer*, Judgment of the Court (Third Chamber) of 7 May 2009, Case C-553/07, paras.23, 42-46, 66-70.

and, where relevant, the data in the legal analysis contained in the minute are 'personal data' within the meaning of that provision, whereas, by contrast, that analysis cannot in itself be so classified. In those circumstances, extending the right of access of the applicant for a residence permit to that legal analysis would not serve the DPD's purpose of guaranteeing the protection of the applicant's right to privacy concerning the processing of data relating to him, but would serve the purpose of guaranteeing him a right of access to administrative documents, which is not however covered by DPD. Therefore, in so far as the objective pursued by that right of access may be fully satisfied by another form of communication, the data subject cannot derive from either Art.12 (a) of DPD or Art.8(2) of the EU Charter the right to obtain a copy of the document or the original file in which those data appear. To avoid giving the data subject access to information other than personal data relating to him, he may obtain a copy of the document or the original file in which that other information has been redacted.[451]

4.2.3.2. Right to rectification

The GDPR provides for various rights of data subjects that allow them to restrict or have an influence over the processing activities carried out by the controller because data processing can negatively affect the rights and freedoms of data subjects, especially when it is illegal or involves inaccurate or incomplete data. These rights include the right to rectify information, erase it, and restrict how it is processed. They must exist in cases where the retention of inaccurate or incomplete data violates the GDPR or other applicable EU or EU MS laws. Therefore, the main purpose of these rights is to stop legal infringements.[452]

As for the right to rectification, the data subject should have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject should have the right to have incomplete personal data completed, including using providing a supplementary statement.[453]

---

[451] *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S*, Judgment of the Court (Third Chamber), 17 July 2014, Joined Cases C-141/12 and C-372/12, paras.20, 46,58-59

[452] Paul Voigt & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Switzerland, Springer International Publishing AG 2017, 154.

[453] Regulation (EU) 2016/679, OJL 119, Art.16.

In *Nowak's case*, Mr Nowak was a trainee accountant who passed first-level accountancy examinations, but failed the later examinations and submitted the data access request to 'the CAI'. The CAI sent 17 documents to Mr Nowak but refused to send him his examination script, on the ground that it did not contain personal data, within the meaning of the data protection legislation. It was however necessary to determine whether the written answers provided by a candidate at a professional examination and any comments made by an examiner toward those answers constitute information relating to that candidate, within the meaning of Art.2(a) of DPD. Accordingly, if information relating to a candidate, contained in his or her answers submitted at a professional examination and in the comments made by the examiner to those answers, were not to be classified as 'personal data', that would have the effect of entirely excluding that information from the obligation to comply not only with the principles and safeguards that must be observed in the area of personal data protection, and, in particular, the principles relating to the quality of such data and the criteria for making data processing legitimate, established in Articles 6 and 7 of DPD, but also with the rights of access, rectification and objection of the data subject. Further, it is clear that the rights of access and rectification, provided for in DPD, may also be asserted concerning the written answers submitted by a candidate at a professional examination and any comments made by an examiner to those answers. Of course, the right of rectification provided for in DPD cannot enable a candidate to 'correct', a posteriori, answers that are 'incorrect'. On the other hand, there might be situations where, for example, because, by mistake, the examination scripts were mixed up in such a way that the answers of another candidate were ascribed to the candidate concerned, or that some of the cover sheets containing the answers of that candidate are lost, so that those answers are incomplete, or that any comments made by an examiner do not accurately record the examiner's evaluation of the answers of the candidate concerned. In so far as the written answers submitted by a candidate at a professional examination and any comments made by an examiner to those answers are therefore liable to be checked for, in particular, their accuracy and the need for their retention, within the meaning of DPD, and may be subject to rectification or erasure, under DPD. The Court must hold that to give a candidate a right of access to those answers and to those comments, under DPD, serves the

purpose of that directive of guaranteeing the protection of that candidate's right to privacy concerning the processing of data relating to him.[454]

4.2.3.3. Right to erasure (right to be forgotten)

The concept of the 'right to be forgotten' received media attention after the CJEU decision in the *Google Spain case* (C-131/12), which was subsequently supported by various academics, scholars, and experts in their research work. On May 13, 2014, in the case of *Google Spain case*, the CJEU had to determine whether for purposes of protection of individuals, the processing of personal data carried out by a search engine operator could be considered as a 'controller,' and whether a data subject's request for deletion of personal data from the list of results could be granted. On the first inquiry, the CJEU decided that, since search engines played a decisive role in the dissemination of information, depending on the type of activities (promotion and sale of advertising space) and establishment (branch or subsidiary) in the MS, the operators of search engines in the processing of personal data should be interpreted as 'controller', but only that it be carried out 'in the context of the activities' of the establishment. This territorial scope of the DPD under Art.4(1) was later reflected in Art.3(1) of the GDPR. About the second matter, on the protection of individuals in the processing of personal data and on the free movement of such data, after a query by a data subject, even initially lawful processing of accurate data may, over time, become incompatible with the DPD and be inadequate, irrelevant or no longer relevant, or excessive concerning purposes of the processing at issue carried out by the operator of the search engine, the information and links concerned in the list of results must be erased.[455] However, Advocate General (AG) Jääskinen weighed that the DPD does not provide for a general 'right to be forgotten' in the sense that a data subject is entitled to restrict or terminate the dissemination of personal data that he considers to be harmful or contrary to his interests. For the sake of completeness, it is useful to recall that the Commission Proposal for a GDPR

[454] *Peter Nowak v Data Protection Commissioner,* Case C-434/16, paras.49-59.
[455] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,* Judgment of the Court (Grand Chamber), Request for a preliminary ruling from the Audiencia Nacional, Case C-131/12, 13 May 2014, 1-21.

provides in its Art.17 for a right to be forgotten.[456] Although the 'right to be forgotten' was first mentioned by the AG, in his opinion, from the new proposed GDPR, the Court, referring to this new concept, did not mention it in its final judgment.

As the right to erasure (right to be forgotten), the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay. At the same time, the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: a) the personal data are no longer necessary to the purposes; b) the data subject withdraws consent; c) the data subject objects to the processing under Art.21(1), 21(2); d) the personal data have been unlawfully processed; e) the personal data have to be erased for compliance with a legal obligation in Union or MS law to which the controller is subject or f) the personal data have been collected about the offer of information society services referred to in Art.8(1). Where the data controller has made personal data public and is therefore required to erase the personal data, the controller, having regard to the available technology and the cost of implementation, must take reasonable steps. These steps include the technical measures, to inform controllers who are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. However, there are exceptional situations in which the right to be forgotten by data subjects is not specifically required in the following cases: a) for exercising the right of freedom of expression and information; b) for compliance with a legal obligation or the performance of a task carried out in the public interest or the exercise of official authority vested in the controller; c) for reasons of public interest in the area of public health; d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes under Art.89(1) or e) for the establishment, exercise or defence of legal claims.[457]

Inevitably, the right to be forgotten sparked a lot of contentious discussions and arguments in the fields of law, philosophy, social work, human rights, and computing. However, because it conflicts with other rights and protected interests, the right to be forgotten has encountered strong opposition from both businesses and advocates of free expression. They questioned the regulation's motivations and stressed the challenge of striking a delicate

[456] Opinion Of Advocate General Jääskinen delivered on Case C-131/12 Google Spain SL Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González, 25 June 2013, para.110-111.
[457] Regulation (EU) 2016/679, OJL 119, Art.17.

balance between the rights at issue, including the right to privacy and the right to freedom of expression, both of which are also protected by the European Convention on Human Rights (Art.10).[458]

Insofar as the data subject has the right to request that the controller erase their personal data, the controller is obligated to do so. Right and obligation are therefore related. In this regard, it is important to keep in mind that the data subject's right only serves to enforce the controller's obligation to erase personal data that would have already existed under one of the grounds listed in Art.17(1) GDPR. Regarding the burden of proof for the existence of a right to erasure, the relationship between the matching right and obligation becomes significant. The data subject must prove the existence of their right to erasure because it is a subjective right. Given that it may need to provide extra evidence under some of these provisions (Art.17(1)a, b,)), the data subject should be required to identify the provision under which it seeks to exercise its rights. The controller would be required to demonstrate favourable conditions, such as by providing counter-evidence to refute any unlawful processing following GDPR Art.17(1) d)).[459]

Enforcing the right to be forgotten is primarily about encroaching on freedom of expression. In *Google Spain*, Google's role as an instrument of freedom of expression was not recognized, but rather economic interests were taken into account. In this case, the CJEU upheld the legitimate interest of potentially interested Internet users in having access to that information, in particular between that interest and the fundamental rights of the data subjects. The CJEU agreed that, in principle, the rights of the data subject protected by the articles in general overrule. The CJEU pointed out that the interests of Internet users, that balance, may in certain cases depend on the nature of the information in question and their sensitivity to the data subject's private life. But also, the CJEU pointed out that this is sometimes in the interest of the public in this information, an interest that can vary in particular depending on the role that the data subject plays in public life. However, in the interest of a fair balance between the interest stakes, the CJEU should take into account Google's role as the publisher of websites about its freedom of expression.[460] Perhaps that is why the GDPR (Art.85) leaves it up to the

[458] Politou et al., *Privacy and Data Protection Challenges in the Distributed Era,* 32-34
[459] Voigt & von dem Bussche, *The EU GDPR: A Practical Guide,* 159.
[460] *Google Spain SL and Google Inc. v Agencia* Española de Protección de Datos (AEPD) and Mario Costeja González., Case C-131/12, para.1-21.

MS to reconcile the right to protection of personal data with the right to freedom of expression and information, which would apply differently depending on the national legal system.

4.2.3.4. Right to restriction of processing and notification obligation

The GDPR introduces the concept of the right to restriction of processing, which is a novel concept. This right permits the temporary halting of the processing of personal data while waiting for the granting of other, more established data subject rights (in particular, the right to rectification and the right to object). In some ways, this right could be seen as a fundamentally adjunct right, closely connected to the exercise of other, more established data subject rights. Therefore, the most important consequence of using the right to restriction of processing is that it can prohibit the deletion of personal data that would otherwise have been lawfully deleted.[461]

As the right to restriction of processing, Art.18 of GDPR provides the data subject should have the right to obtain from the controller restriction of the processing. This right to restriction applies when a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; c) the controller no longer needs the personal data for purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; and d) the data subject has objected to processing under Art.21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject. Where processing has been restricted, such personal data should, with exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or the protection of the rights of another natural or legal person or reasons of important public interest of the Union or of the MS. A data subject who has obtained a restriction of processing under this paragraph 1 of Art.18 should be informed by the controller before the restriction of processing is lifted.[462] It is vital

[461] Gloria González Fuster 'Article 18. Right to restriction of processing' in Christopher Kuner, Lee A. Bygrave and Xe Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary*, New York, Oxford University Press, 2020, 486-487.
[462] Regulation (EU) 2016/679, OJL 119, Art.18.

to emphasise that if the data subjects are informed about the lifting process before the lifting itself, they may have more options to consider or rights to exercise before the de-selection or deletion of the data.

In the *Google Spain* case, the CJEU also mentioned that since the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the EU Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name.[463] This repeats the methods of the restriction of personal data which was mentioned in Rec.67 of GDPR. Methods for restricting the processing of personal data may include but are not limited to, temporarily moving selected data to another processing system, preventing users from accessing selected personal data, or temporarily removing published data from the website. In automated filing systems, the restriction of processing should in principle be secured by technical means so that personal data are not subjected to further processing and cannot be changed. It must be indicated in the system the fact of restriction of processing of personal data.[464]

According to Art.4(3) of the GDPR, there is a restriction of processing which refers to the marking of personal data that has been stored with intention of limiting its processing going forward. However, Art.18 of the GDPR omits any mention of marking in favour of defining the effects of gaining the right to restriction as the limitation of the potential justifications for further processing of such data. The controller must communicate any rectification or erasure of personal data or restriction of processing carried out following Art.16, Art.17(1) and Art.18 to each recipient to whom personal data have been disclosed unless this proves impossible or involves disproportionate effort. The controller must inform the data subject of these recipients if the data subject requests it.[465] Nevertheless, what needs to be communicated to recipients is not exactly specified in the GDPR, but probably, it could

[463] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,* Case C-131/12, para. 99
[464] Regulation (EU) 2016/679, OJL 119, Rec. 67.
[465] Ibid, Art.19.

be the rectification or erasure of personal data or restriction of data processing that has been carried out.

The right to restriction of processing has not received much attention either in academia or in the legal policy discussion. Perhaps one of the explanations is that the GDPR defines the right to restriction of processing as both a right of the data subject and a powerful measure of the supervisory authorities under Art.58(1)(g). The other confusing point would be that traditionally, after the term 'restriction', the first thing that comes to mind is the restriction of the permissible rights of the data subjects. However, as in a new right, the term 'restriction' refers to restrictions that limit data processing of personal data and can therefore create ambiguity. The culmination of this ambiguity creates even more confusion when Rec.73 of the GDPR refers to restrictions on data protection principles and data subject rights, rather than the right to restriction of data processing.

Art.19 does not mention the potential need for data controllers to inform recipients who have received a notice of restriction of processing of the possible lifting of such restriction, although they are still required to inform data subjects of this. In this case, data subjects are responsible for informing misinformed recipients immediately in such circumstances. Since the controller, at the request of data subjects, must also inform them 'about those recipients', it is not clear whether 'those recipients' refers to all recipients to whom personal data was disclosed, or only to those who were essentially notified. It is presumed that the data subject is particularly interested in knowing exactly whose recipients may have the data, rather than those who have been notified for potential future communication. In addition, Art.19 is vague as to whether recipients should communicate data subjects before or after recipients have received notification, which can be challenging in some circumstances.

4.2.3.5. Right to data portability

The brand-new data subject right made possible by the GDPR is the right to data portability. Although it is still relatively new in terms of usage, it may be the pinnacle of giving the data subject control over their personal information because it allows them to receive it from the controller and communicate it to another controller. The right to data portability can be used in conjunction with the right to erasure in Art.17, which means that

the data subject can stop further processing of their personal information by the controller in addition to receiving it from the controller. The right to portability also aids in demonstrating another point, namely that the controller does not actually possess the personal data that they process in the sense of having property rights therein, but rather that the law merely grants them a licence to use the data under the condition that they fully adhere to the GDPR's requirements. The data subject effectively revokes that licence by using both the right to portability and the right to erasure.[466]

Individuals who exercised their right to access information under the DPD 95/46/EC were limited by the format the data controller chose to use for providing the requested information. As it makes it easier for data subjects to move, copy, or transmit personal data from one IT environment to another, the new right to data portability aims to provide data subjects more control over their personal data, whether it is in their systems, the systems of trusted third parties or those of new data controllers. Data portability gives a chance to 're-balance' the relationship between data subjects and data controllers by reaffirming individuals' personal rights and control over personal information about them. The GDPR regulates personal data, not competition, even though the right to personal data portability may increase competition between services, by easing service switching.[467]

According to Art.20 of GDPR, the right to data portability is in which the data subject should have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. The right to portability applies only in certain circumstances, such as where a) the processing is based on consent under point (a) of Art.6(1) or point (a) of Art.9(2) or on a contract under point (b) of Art.6(1), and b) the processing is carried out by automated means. In exercising his or her right to data portability under paragraph 1 of Art.20, the data subject should have the right to have personal data transmitted directly from one controller to another, where technically feasible. The exercise of the right referred to in paragraph 1 of Art.20 should be without prejudice to Art.17. That

[466] Stewart Room 'The rights of data subjects' in Stewart Room (ed) *Data Protection and Compliance*, Swindon, UK, BCS Learning and Development Ltd, 2021, 309.
[467] Article 29 DPWP, 'Guidelines on the right to data portability', adopted on 13 December 2016, as last Revised and adopted on 5 April 2017, 16/EN WP 242 rev.01, 4.

right should not apply to processing necessary for the performance of a task carried out in the public interest or the exercise of official authority vested in the controller. The right referred here should not adversely affect the rights and freedoms of others.[468] There is no case law relevant to the right to data portability because the DPD lacks an antecedent to the right to data portability.

The ability to receive personal information about oneself that has been provided to a controller in a structured, commonly used, machine-readable, and interoperable format and to transmit it to another controller would help the data subject maintain even more control over the processing of his or her information when it is done so automatically. The creation of interoperable formats that support data portability should be fostered by data controllers. When the data subject gave the personal information with their consent or the processing was required to carry out a contract, that right should be applicable.[469] It is not clear how these requirements might be balanced about the norms for a commonly used and interoperable format. The wide phrasing provides for the provision's independence from technological change, but the EU legislators make no hints in that regard. However, the widespread application of a format should be decided based on the level of the technology, which, for example, would be satisfied by PDF or Office formats.[470]

The right to portability of the data subject is made up of different components. The initial component of data portability is the data subject's right to receive a portion of the personal data about him or her that has been processed by a data controller and to keep that data for later personal use. Without necessarily sending the data to another data controller, such storage can take place on a private device or in a private cloud. Furthermore, Art.20(1) grants data subjects the freedom to transfer their personal data 'without hindrance' from one data controller to another. In cases where it is technically possible and the data subject requests it, data may also be transferred directly from one data controller to another (Art.20(2)). In this regard, Rec.68 encourages data controllers to create interoperable formats that support data portability without imposing a need that controllers to use or maintain technically comparable processing systems. However, the GDPR forbids controllers from putting up obstacles to transmission. Essentially, this aspect of data portability gives data

[468] Regulation (EU) 2016/679, OJL 119, Art.20.
[469] Ibid, Rec. 68.
[470] Voigt & von dem Bussche, *The EU GDPR: A Practical Guide*, 174.

subjects the ability to retrieve, reuse, and transmit the information they have provided to another service provider or either within the same business sector or in a different one. The right to data portability is supposed to encourage opportunities for innovation and the safe and secure interchange of personal data between data controllers under the authority of the data subject, in addition to empowering consumers by eliminating 'lock-in'. Data portability can encourage consumers to share their personal information in a controlled and limited way between organisations, enhancing services and customer experiences. The portability of data may make it easier for users to share and reuse their personal information across the numerous services they are interested in. Controllership over the data subjects of the personal data is the final component of the right to portability. The right to obtain and use personal information following the preferences of the data subject is guaranteed by data portability. Under the circumstances outlined in Art.20, data controllers who respond to requests for data portability are not liable for the processing carried out by the data subject or by another business that receives personal data. They represent the data subject in all situations, even when the personal data are sent directly to another data controller. Given that it is not the sending data controller that selects the recipient, the data controller is not accountable in this regard for the receiving data controller's compliance with data protection law. The controller should also put in place safeguards to make sure they truly act in the data subject's best interests. In responding to a request for data portability, data controllers are not required to evaluate and validate the accuracy of the data before sending it.[471]

The form of the transferred data is not mentioned in Art.20 of the GDPR, other than the need that it be 'machine-readable,' which is not explained. Additionally, since 'technically feasible' is also not defined under the GDPR, it may appear that a direct data transfer from one controller to another is not practicable. However, from a legal standpoint, the data controllers may need to adapt to new cutting-edge technology for direct controller-to-controller data transfers to be successful.

4.2.3.6. Right to object

[471] Article 29 DPWP, 'Guidelines on the right to data portability', 4-6.

As the right to object, the data subject should have the right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her which is based on point (e) or (f) of Art.6(1), including profiling based on those provisions. The controller should no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. It can be assumed that this is a general right of the data subject to object, while it can be seen from the provisions of the GDPR that there is another type of more specific right to object, such as the right of the data subject to object to direct marketing. If personal data is processed for direct marketing purposes, the data subject has the right to object at any time to the processing of personal data concerning him for such marketing, including profiling, insofar as it is related to such direct marketing. If the data subject objects to the processing for direct marketing purposes, the personal data would no longer be processed for such purposes. At the latest during the first communication with the data subject, the right referred to in paragraphs 1 and 2 of Art.21 must be expressly communicated to the data subject and must be presented clearly and separately from any other information.[472]

In the *Google Spain case*, in addition to the right to erasure (the right to be forgotten) of Art.12(b) DPD, the right to object under Art.14(a) DPD also had to be considered in determining the scope of the questions. Whilst the question of whether the processing complies with Articles 6 and 7(f) of the DPD may be determined in the context of a request as provided for in Art.12(b) of the DPD, the data subject may, in addition, rely in certain conditions on the right to object laid down in Art.14(a) of the DPD. Under Art.14 (a) of DPD, MS are to grant the data subject the right, at least in the cases referred to in Art.7(e) and (f) of the DPD, to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. The court also emphasised that the balancing to be carried out under Art.14(a) thus enables account to be taken in a more specific manner of all the circumstances surrounding the data subject's particular situation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data.[473]

[472] Regulation (EU) 2016/679, OJL 119, Art. 21.
[473] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,* Case C-131/12, para.75-76.

4.2.3.7. Right not to be subject to a decision based on automated individual decision-making, including profiling

Art.22 of GDPR provides that the data subject should have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him/her or similarly significantly affects him/her. Profiling is subject to GDPR rules governing the processing of personal data, such as the legal basis for processing or data protection principles. The European Data Protection Board (Board), established under the GDPR should be able to make recommendations in this context. According to GDPR, 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. However, the data subject's right not to be subject to a decision based on automated processing, including profiling should not apply if the decision: a) is necessary for entering into or performing a contract between the data subject and a data controller; b) is authorised by EU or MS law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests or c) is based on the data subject's explicit consent. In the cases referred to in points (a) and (c) of paragraph 2 of Art.22, the data controller must take appropriate measures to protect the rights and freedoms and legitimate interests of the data subject, at least the right to obtain human intervention on the part of the controller to express his point of view and challenge the decision.[474]

A growing number of industries, both public and private, are using automated decision-making and profiling. Profiling is being used more frequently to support decision-making in a variety of industries, including banking and finance, healthcare, taxation, insurance, marketing, and advertising. Big data analytics, AI and ML skills have made it simpler to develop profiles and make automated choices, which have the potential to have a substantial impact on people's rights and freedoms. Both individuals and organisations can profit from

[474] Regulation (EU) 2016/679, OJL 119, Art. 22.

profiling and automated decision-making, which can result in advantages like a) higher productivity and b) resource savings. However, the rights and freedoms of persons can be seriously jeopardised by profiling and automated decision-making, necessitating suitable protections. These procedures could be hazy. People might not be aware that they are being profiled or comprehend the implications. Profiling may reinforce existing social divisions and stereotypes. Additionally, it can confine a person to their suggested preferences and lock them into a particular group. This may limit their ability to select, for instance, particular goods or services like books, music, or newsfeeds. Profiling may occasionally result in incorrect predictions. In other situations, it might result in unfair discrimination and the denial of goods and services.[475]

According to general evaluation, the GDPR has successfully achieved its goals of increasing the protection of an individual's right to personal data protection and ensuring the free movement of personal data within the EU two years after it began to be applied. There are, however, a few areas that could use development in the future. The Commission agrees with the majority of stakeholders and DPAs that it would be premature at this time to make firm judgments on how the GDPR is being applied. It is expected that as the GDPR is applied more frequently over the ensuing years, the majority of the difficulties raised by MS and stakeholders will be resolved. However, there is a report outlining the difficulties that have been encountered thus far in implementing the GDPR and suggesting potential solutions.[476]

However, some areas still require development. To begin with, not all data controllers uphold their obligation to make it easier for data subjects to exercise their rights. They must make sure that data subjects have a reliable person they can talk to about their issues. This might be the data protection officer, whose contact information must be made available to the data subject in advance. The contact options must allow the data subject to communicate with the controller in additional ways besides only email. Moreover, the potential of the right to data portability is not being fully utilised. The European Strategy for Data (hereinafter Data Strategy), which was adopted by the Commission on February 19, 2020, highlighted the need

[475] Article 29 DPWP, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679', adopted on 3 October 2017, as last Revised and Adopted on 6 February 2018, 17/EN WP251rev.01, 5-6.

[476] European Commission, 'Communication from the Commission to The European Parliament and The Council, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation', Brussels, 24.6.2020, COM (2020) 264 final, 4.

to make it easier for all potential uses of this right, such as by requiring technical interfaces and machine-readable formats that permit data portability in (near-to) real-time. Operators observe that due to the lack of a standard, it can occasionally be challenging to provide the data in an organised, widely used machine-readable manner. In addition to data portability, new technology tools have been created to make it easier for people to exercise their GDPR rights, such as personal data spaces and personal information management services. In regards to children's rights, several members of the Multi-Stakeholder Group emphasise the necessity to inform children and the reality that many organisations fail to consider how processing their data may affect children. The Council emphasised that while creating standards of conduct, special consideration could be given to child protection. Authorities in charge of data protection also prioritise protecting children. Additionally, some businesses take a very legalistic approach to the right to information, treating data protection notices like a legal exercise and providing information that is overly complicated, imprecise, or both. However, the GDPR dictates that all information should be brief and written in plain language. It appears that certain businesses do not abide by the Board's guidelines, for instance when it comes to disclosing the identities of the organisations, which they share data with. Lastly, several MS severely limited the rights of data subjects through national law, some even going beyond what is permitted under Art.23 of the GDPR. The activities of a few significant digital actors occasionally pose a challenge for individuals to select the settings that best safeguard their privacy, which restricts their ability to exercise their rights.[477]

The GDPR ensures that data privacy laws are applied consistently across the EU. However, it gives MS the option to further define the GDPR in some areas while requiring them to legislate in others. As a result, there is still some fragmentation, which is especially because facultative specification clauses are used frequently. Children and their parents may be uncertain about how their data protection rights would be applied in the Single Market due to differences between MS in the age at which children must agree to the use of information society services. Additionally, this fragmentation makes it difficult to innovate and execute

[477] European Commission, 'Commission Staff Working Document Accompanying the document Communication from the Commission to the European Parliament and the Council Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, Brussels, 24.6.2020, SWD (2020) 115 final, 20-21.

cross-border business, particularly regarding new technological advancements and cybersecurity solutions.[478]

4.2.4. Summary

The advent of the GDPR as the new digital regulation has introduced a new generation of data protection regulations to all EU users and, in general, to all users worldwide. The GDPR is enforceable and applicable to all the EU MS since it protects information privacy and other fundamental human rights against the hazards of processing personal data. The GDPR alters the technological, economic, societal, political, and entrepreneurial climates of businesses, as well as the stages of data processing for SMEs. The processing of data subjects' personal data has changed as a result of these advances, with a focus on the data subject's ability to effectively exercise their digital rights and control over their personal data. Due to the significant impact of the GDPR on the protection of individuals' personal data during processing, existing privacy-security-related regulatory frameworks such as the e-Privacy and NIS Directives have to be redesigned and revised to keep up with the most recent technological developments.

It is worth noting that the GDPR protects personal data, whereas the anticipated e-Privacy Regulation would safeguard the confidentiality of e-communications and devices. While the GDPR applies all personal data regardless of how it is transmitted, the e-Privacy Regulation would regulate e-communications and the integrity of the data on a user's device, regardless of whether the data is personal or not. The GDPR defines the right to the protection of personal data, but the e-Privacy Regulation would deal with the right to privacy and confidentiality of communications. The GDPR has introduced new rights for citizens and obligations for companies, the e-Privacy regulation would ensure that mobile applications or internet services through which users communicate cannot be intercepted, recorded, listen or listened to their communications. The GDPR began to apply on May 25, 2018, but the e-Privacy regulation was proposed on January 10, 2017, and is currently in the legislative process in the European Parliament and the Council.

[478] European Commission, 'the EU's approach to the digital transition - two years of application of the General Data Protection Regulation', COM (2020) 264 final, 7.

However, some provisions in the GDPR would have to be criticized for further better implementation. When processing the personal data of children, the GDPR does not explicitly state who should submit a request for access to information. So, allegedly children themselves can submit a request for access to information. But there is still no answer to what extent and up to what age child data subjects can submit a request for access to information and even to communication. Since private law regulates legal liability differently in the MS, the fulfilment of these requirements will depend on national legal systems.

4.3. The concept of vulnerable individuals in the EU data protection law

It will be useful to examine the concept of vulnerability from the perspective of data protection law, especially in the GDPR, after briefly explaining the interaction between consumer protection and data protection laws concerning the position of individuals in these two mechanisms, both as a consumer and as a data subject.

Consumer law and data protection law were once considered to be two separate fields of law. Consumers and their interactions with sellers of goods and services are at the heart of consumer law. Consumer law gives consumers enforceable rights to level the playing field for business dealings. By processing personal data, data protection law seeks to uphold equity and fundamental rights. Fair contracting is covered by consumer law, and fair processing is covered by data protection law. These worlds begin to converge in a digital economy. Several online digital services are being provided in exchange for personal data rather than actual money. The concept of paying with data has gained popularity but is inaccurate. Many new smart data-driven consumer products and services depend heavily on data, and as the Internet of Things spreads, the need of collecting and processing data as part of providing services to customers will only grow. The line between consumer law and data protection law is blurred in data-driven consumer markets. As consumer products incorporate more and more data, many data privacy issues also affect consumers and vice versa.[479]

The interaction of consumer and data protection rules appears very logical at first glance. This is because the two regimes are already convergent in reality, in the creation of

[479] Natali Helberger et al., 'The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law' *Common Market Law Review,* vol.54/5, 2017, 1-2.

EU policy, and EU law. The protection of consumers' personal data is a crucial component of consumer protection because the roles of consumers and data subjects are inextricably linked in the digital world. However, on a broader scale, consumer protection and data protection have a lot in common: both are recognised in the EU Charter, have their origins in the national laws of the MS, and were created as rights starting with secondary EU legislation. These legal disciplines both often work to protect weaker parties – consumers and data subjects, who are frequently perceived as behaving inherently unequally powerful ways and possessing asymmetric knowledge.[480]

European consumer and personal data protection regulations offer a solution to related legal problems since they both seek to give a minimal level of protection to individual human beings operating in the marketplace - consumers and data subjects. First of all, it would be important to emphasise that the CRD and GDPR are intended to safeguard the weaker subject. In reality, it is thought that consumers and data subjects are much weaker than their counterparts, traders and data controllers, and they typically are. It is common knowledge that regarding B2C contracts, the trader acts for trade, business, craft, or professional interests. While consumers only act for personal reasons, traders can draw on their professional experience. Similarly, to this, data subjects frequently have no notion that they are in control of their data, are being profiled, or that a data controller is processing their data. These two subjects engage in online transactions rather than in person, stipulate contracts with a counterpart who is more knowledgeable than they are and deals with a variety of topics, and behave in very similar ways. Nevertheless, in most juridical connections, the consumer and the data subject are indeed the same individuals.[481]

The European Data Protection Supervisor observed in its Preliminary Opinion that the promotion of growth, innovation, and the welfare of individual consumers are among the common goals shared by EU approaches to data protection, competition, and consumer

[480] Milda Mačėnaitė 'Protecting Children Online: Combining the Rationale and Rules of Personal Data Protection Law and Consumer Protection Law' in Mor Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law, MPI Studies on Intellectual Property and Competition Law 28,* Germany, Springer-Verlag GmbH, 2018, 352-353.

[481] Matilde Ratti 'Personal-Data and Consumer Protection: What Do They Have in Common?' in M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law, MPI Studies on Intellectual Property and Competition Law28,* Germany, Springer-Verlag GmbH, 2018, 378-380.

protection.[482] The EU strives for a 'high level of protection' of the economic actions of a data subject who is also a consumer. The goal of data and privacy protection laws and consumer protection laws is the same: to safeguard the autonomy of the natural person (in the market for consumer protection; in a moral sense for data and privacy protection). Nonetheless, the idea of consumer protection is more understandable. Consumer protection explicitly strives to overcome power disparities based on knowledge asymmetries in the market. In contrast to this, the privacy and data protection law involves a complicated balancing of the interests of parties in an infinite number of circumstances. Whereas consumer protection law is based on shared competence, EU data protection law is based on the MS' conferral of competence. Because of this, MS are unable to raise the level of protection offered by EU data protection law unless it is expressly permitted, contrary to consumer protection law, where doing so is permitted without an express prohibition.[483]

It is undeniable that consumers, specifically online consumers, may also be viewed as data subjects insofar as their consumption involves sharing or communicating personal information about them. Also, though, if data concerning an individual is gathered in exchange for free access to online services, that person is increasingly depicted as a consumer. This graphic is used to emphasise the fact that free online services might not be as free as they seem because the personal data obtained through them has a certain financial value. The justification for portraying the data subject in the role of a consumer is thus inextricably linked to the idea that users are often unaware of and confused by the nature of the services they use, misinterpreting their behaviour as a result. In this regard, some data subjects seem to be ignorant to the point where they misunderstand how exactly internet services work, which causes them to engage in careless data practices.[484]

4.3.1. The concept of the average data subject in the EU data protection law

[482] European Data Protection Supervisor, 'Preliminary Opinion of the European Data Protection Supervisor, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy', Brussels, 2014, 3.
[483] Michiel Rhoen, 'Beyond consent: improving data protection through consumer protection law', *Internet Policy Review*, vol.5/1, 2016, 6-8
[484] Gloria González Fuster, 'How Uninformed is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection', *Revista de Internet: Derecho y Política*, vol.19, 2014, 99.

Indirectly, the term 'data subject' is defined in the GDPR in Art.4(1), which specifies that 'personal data' refers to any information belonging to an identified or identifiable natural person. So, the identified or identifiable natural person to whom personal data pertains is the data subject.[485] There is no mention of the primary attributes of this legal figure, albeit one could attempt to extrapolate these primary attributes from the other GDPR. The GDPR requires data controllers to inform data subjects of their rights whenever they collect data from them, therefore in this case, it would seem that the data subject is, in theory, someone who is unaware of the existence of their data protection rights. Yet, in theory, it is still envisaged that data subjects will be able to give informed consent after being given certain information. As many academics assert, the emphasis on information responsibilities in the discourse on data protection assumes that there is a rational, informed data subject who takes deliberate decisions. The emphasis on consent, as the result of the data subject's rational and informed decision-making process, reflects the same methodology. It is interesting to note that the average data subject was repeatedly mentioned in the Commission's first proposal for the DPD. In other words, the legislator was counting on the data subject's rational decision-making abilities, who can weigh the pros and cons of data processing and make well-informed choices about it. This appears to be comparable to the consumer who can make intelligent choices and who is reasonably informed, observant, and circumspect, as claimed in the consumer law acquis. This reliance on an average and reasonable data subject, modelled after the rational consumer in the EU consumer legislation, has not lessened but risen with the transition from the DPD to the GDPR. The GDPR appears to be based on the notion that all data subjects are rational actors that will carefully consider and evaluate the implications of consent and read all privacy declarations.[486]

Several significant discussions between the concept of the data subject and how the data subject functions under the EU law are made clear by using the benchmark of the average consumer. First and foremost, it appears incredibly challenging to argue that EU legislation considers the data subject to be informed by default. However, one of the fundamental premises underlying the development of personal data protection law is that people either lack enough information about data processing activities that impact them or are in danger of

[485] Regulation (EU) 2016/679, OJL 119, Art.4.
[486] Gianclaudio Malgieri & Gloria Gonzalez Fuster, 'The vulnerable data subject: A gendered data subject?' *European Journal of Law and Technology*, vol 13(2), 2022, 1-26.

losing control over their data. The initial and general lack of information for data subjects seems to be significant. If people receive some pieces of information, the processing of the personal data may be considered fair, and they will be able to promptly decide whether to consent to certain practices, but generally speaking, they are still largely in the shadows. More crucially, identifying what constitutes a 'standard notion of the data subject'- someone who has access to information and the capacity to make decisions, appears to be a requirement for defining which online practices are unlawfully misleading. It is striking that despite the importance of the data subject's right to know and the information requirements placed on data controllers for European personal data protection, there is no specific benchmark in the EU law as to the degree of data subject misinformation that should be regarded as unlawful.[487]

Categories of data subjects or records containing personal data are not defined by the GDPR. To refer to the numerous groups of people whose personal data has been compromised, WP29 offers the other following categories of data subjects which could include, among others, children and other vulnerable groups, individuals with disabilities, employees, or customers, depending on the descriptions employed. Similar to categories of financial records, categories of personal data records can refer to the various record types that the controller may process, such as health information, educational information, social services information, financial information, bank account information, passport information, and so forth.[488]

Data subjects are not all the same, so it is feasible to identify differences based on their standing and treatment concerning data protection law. The protection of the data subject's rights and the data subject's ability to act as such, following the possibilities defined by the law, appear to be the two key viewpoints that are relevant when evaluating whether this is expedient. The data controller is required to abide by the regulations concerning all types of personal data and to protect all data subjects regardless of who they are, therefore there may be no reason to create distinctions when it comes to the protection of the rights of the data subject. Although it should go without saying, it should be acknowledged that some data subjects are more vulnerable than others and that the controller should take this into account when processing data. This is especially true when it comes to the fundamental concepts of

[487] Fuster, 'How Uninformed is the Average Data Subject', 101.
[488] Article 29 DPWP, 'Guidelines on Personal data breach notification under Regulation 2016/679', adopted on 3 October 2017, as last revised and adopted on 6 February 2018, 18/EN/WP250rev.01, 14.

fairness and proportionality. Personal data should be processed with caution when the data subject is vulnerable or put in a precarious position, depending on the circumstances. Specific regulations on the processing of data about various categories of data subjects are probably not necessary, but the fairness principle might be expanded upon and supplemented with a care principle. Such a principle might usually compel the controller to consider the characters of the data subject when enforcing particular laws. As a result, if this point is overlooked, data processing can be viewed as illegal. There may be more types of data subjects that may be listed, however, the term 'data subject' does not have a unified standard notion. Some data subjects don't have the full legal ability for a variety of reasons. This is a troubling finding since it points to a flaw in the data protection law and raises the issue of whether its core goal of protecting privacy and integrity can be achieved. Although it is clear that issues exist, the practice of supervisory agencies through their unique rulings could make data protection more nuanced.[489]

4.3.2. The concept of vulnerability in the EU data protection law

Exposure to unfavourable forces just as emotional, physical, or otherwise is referred to as vulnerability. On the other hand, this seems to stretch the definition of vulnerable. Typically, when it is talked about someone being vulnerable, it meant that they are open to harm. Of course, no harm can come to an invulnerable person or group. It is extremely important to understand that vulnerability is not binary. Following various authors, the first understanding is that no one is completely invulnerable at all times and in all situations, but everyone is susceptible to varying degrees and under different conditions. The next realization is that vulnerability is not solely the result of chance. The vulnerability itself can be engineered or controlled in the same way that the conditions that lead to it can. Vulnerability is not, or at least not entirely, a phenomenon that happens in nature. A person, a group, or a society may take advantage of any vulnerability that arises in the world. For example, an unscrupulous carer may take advantage of the vulnerability of an elderly charge to change her

[489] Peter Blume, 'The Data Subject', *European Data Protection Law Review (EDPL),* vol.1, no.4, 2015, 259.

mind. Separately, however, a person, group, or society may increase a person's vulnerability by exposing them to certain events, behaviours, or facts.[490]

For researchers and enterprises that offer users digital tools and infrastructure, designing privacy for users pose significant hurdles. Yet, recent research on technology and privacy has revealed what has been assumed or known about vulnerable groups: networked technologies frequently duplicate (or exacerbate) the inequalities that make offline people vulnerable. Vulnerable populations are defined by the authors as groups of people who are more likely to experience privacy intrusions due to their race, class, gender, sexual orientation, religion, or other intersectional traits or circumstances.[491]

Some academic authors[492][493] believe that *Luna's* layered theory of vulnerability is successful because it can address both the problems with vulnerability as a label, such as the potential for stigmatisation and the problems with universal vulnerability, such as the danger that if everyone is vulnerable, the idea will no longer be effective in defending weaker people. The layered understanding of vulnerability can help clear up some confusion between harm-based and procedural methods and offer some confidence in mitigation strategies. In a recent study on layers of vulnerability, *Luna* attempted to operationalise the idea and put out a technique for recognising and evaluating various degrees of risk. In particular, *Luna* advises evaluating vulnerability risks by taking into account both the likelihood of hazards and the harmfulness of impacts.[494]

A new area of discussion in the regulation of digital markets is individual vulnerability. However, it can be seen in the fragmented protection of various kinds of individual vulnerabilities within EU legislation: consumer protection law takes into account vulnerable consumers in the regulation of unfair business practises[495]; other industry-specific EU

[490] Ryan Calo, 'Privacy, Vulnerability, and Affordance', *DePaul L.aw Review,* vol.66, 2017, 592-594.
[491] Nora McDonald & Andrea Forte 'Privacy and Vulnerable Populations' in B. P. Knijnenburg et al. (eds.), *Modern Socio-Technical Perspectives on Privacy,* Switzerland, Springer Nature, 2022, 338.
[492] Gianclaudio Malgieri & Jedrzej Niklas 'Vulnerable data subjects', *Computer Law & Security Review,* vol.37, 2020, 105415, 2.
[493] Gennet et al., 'Does the new EU Regulation on clinical trials adequately protect vulnerable research participants?' *Health Policy*, vol.119, 2015, 925–931.
[494] Florencia Luna, 'Elucidating the Concept of Vulnerability: Layers Not Labels', *International Journal of Feminist Approaches to Bioethics*, vol.2, 2009, 121.
[495] Directive 2005/29/EC, OJ L 149, 22–39.

provisions address vulnerable workers[496], vulnerable road users[497], and vulnerable research participants in clinical trials.[498] Even though the GDPR and data protection law, in general, do not explicitly protect vulnerable data subjects, the issue of vulnerability in data protection has sparked a lively discussion. Yet, from both a theoretical and a practical standpoint, it seems that efforts to identify and protect vulnerable individuals in the context of data protection law and associated fields, which are based on a hazy notion of 'data power' imbalance, are still lacking.[499]

It is important to remember that everyone has the potential to be vulnerable, and that access to resources, such as public services offered in a country and cultural variables impact people's resilience, or their capacity to deal with vulnerability. Above all, it's crucial to keep in mind that people are what vulnerable group members are first and foremost. Any additional definitions - as a citizen, a vulnerable individual, or a data subject - should come in second place to this. Also, vulnerable individuals and groups run the risk of their data being used in ways they may not want or consent to (e.g., refugees who are under greater state surveillance). While this is an issue for all citizens, vulnerable persons may find it harder to prevent this: for example, they may be incapable of granting consent, or may not be proficient in the native language(s) of the country they live in. For vulnerable data subjects, power imbalances between data subjects and data controllers may be amplified. For instance, vulnerable individuals may discover that they have less authority, knowledge, or understanding of the issue in situations where personal data is susceptible to misuse by data controllers, which may limit their ability to manage or prevent this. As persons are grouped or classified (e.g., elderly, immigrant) for the purposes of study and analysis, there is a risk of (increased) stigmatisation. These risks include both the type of personal information being gathered and used as well as how vulnerable a person is. Depending on the location and context in which they are utilised,

[496] Directive 2014/54/EU of the European Parliament and of the Council of 16 April 2014 on measures facilitating the exercise of rights conferred on workers in the context of freedom of movement for workers Text with EEA relevance, OJ L 128, 30.4.2014, p. 8–14, Rec. 5.
[497] Regulation (EU) No 540/2014 of the European Parliament and of the Council of 16 April 2014 on the sound level of motor vehicles and of replacement silencing systems, and amending Directive 2007/46/EC and repealing Directive 70/157/EEC Text with EEA relevance, OJ L 158, 27.5.2014, 131–195.
[498] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC Text with EEA relevance, OJ L 158, 27.5.2014, 1–76.
[499] Gianclaudio Malgieri & Antonio Davola, Data-Powerful, February 5, 2022, 1-3. <https://ssrn.com/abstract=4027370> accessed 15 Aug. 2023.

certain sorts of data, such as details on a person's religion, health history, or sexual orientation, may pose a greater danger.[500]

Scholars studying privacy and data protection have not yet focused much on vulnerability as a concept. In practice, there are two main dichotomies in theories of human vulnerability that can be found significant in the discussion of data protection. The initial distinction is between universality that everyone is equally susceptible and particularity relates to the notion of vulnerable subjects. The second dichotomy relates to manifestations of vulnerability, just as vulnerability may arise either as a result of the processing of the data, like decisional vulnerability risks associated with consent provision, data collection, and improper use of data protection rights or as a result of the processing's results which some data processing may generate discrimination, manipulation or secondary harms such as physical or psychological harms. As a result, privacy and data rights serve as protective measures and generate obstacles to the identification, presentation, and exploitation of those vulnerabilities. However, in practice, there is a great deal of variation in the positions of various data subjects due to their varying levels of awareness, decisional capacity, the propensity to disclose their data and weaknesses. Still, in the discourse surrounding data protection, the idea of a data subject has traditionally been singular and rigid, and it is unclear whether or not such a singular idea refers to an average data subject, like in the field of consumers, or not.[501]

4.3.3. The concept of vulnerable data subjects in the GDPR

The way vulnerable data subjects are conceptualised is loaded with issues. Initially, there is a lack of conceptualisation of the term 'vulnerable data subjects.' These challenges have just lately received more focus within academic personal data protection studies. It appears that specific definitions of vulnerability tend to focus on a problem unique to a certain group, which is then defined through actual implementation. These behaviours or their use appear to put an end to conversations on other forms of vulnerability. It is debatable if the vulnerability is even the proper concept. Moreover, the legal framework does not adopt an

[500] Castańeda Alexandra et al., 'Research Report ICTs, data and vulnerable people: a guide for citizens', *University of the Basque Country (UPV/EHU),* Bilbao, 2021, 11-16.
[501] Malgieri and Niklas, 'Vulnerable data subjects', 2.

intersectional approach; socioeconomic considerations are not taken into account as risk factors for a data subject. Additionally, because of the debates' emphasis on risks, the empowering effects of data gathering and processing are given less consideration. For instance, police registrations can be used to assess the degree of ethnic profiling. Finally, aside from offering advice and guidelines for children, DPAs do not appear to have addressed the issue of vulnerable data subjects in practice.[502]

Fundamentally, there is no explicit definition of vulnerable data subjects in the GDPR. The phrase 'where personal data of vulnerable natural persons, in particular of children, are processed'[503] appears only once in Rec.75 of GDPR concerning relevant risks to take into account when conducting a data protection impact assessment. The GDPR specifically addresses the status of children through conditions to consent in relation to the information society (Art. 8) and transparent information, communication, and modalities for the exercise of children's rights (Art. 12(1)). Where point (a) of Art.6(1) applies and a child is directly offered information society services, then the processing of the child's personal data is permitted under Art.8 if the child is at least 16 years old. If the child is under 16, the processing will only be legal if and to the extent that the person who has parental responsibility for the child gives consent or authorises it. The MS may set a lower age by legislation for such reasons as long as it does not fall below 13 years. Taking into account current technology, the controller should take reasonable measures to verify that permission is granted or authorized by the holder of parental responsibility for the child. Paragraph 1 should not impact normal contract law in the MS, such as regulations governing the validity, formation, or effect of a transaction involving a child.[504] One might conclude that the GDPR's approach to vulnerability is specific and not general - only some groups, namely children, are vulnerable. Children are particularly vulnerable data subjects. Although children are just one group at high risk, the definition of the data subject is universal and distinct, and other groups can typically face similar risks (for example elderly, mentally ill persons).[505]

[502] Jonas Breuer et al., 'Data protection as privilege: Factors to increase meaning of GDPR in vulnerable groups', *Frontiers in Sustainable Cities*, vol.4, 2022, 03.
[503] Regulation (EU) 2016/679, OJ L 119, 1–88.
[504] Regulation (EU) 2016/679, OJL 119, Art.8.
[505] Malgieri and Niklas, 'Vulnerable data subjects', 2.

The GDPR also mentioned in Rec.38 that children merit specific protection concerning their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights to the processing of personal data. The use of children's personal information for marketing or the creation of personality or user profiles, as well as the acquisition of personal information about children when utilising services that are made specifically for children, should fall under this additional protection. When preventative or counselling services are provided directly to a child, the approval of the person with parental responsibility should not be required. Children deserve special care, thus all information and communication that is directed at them should be written in language that is simple and easy to understand by them.[506]

In other words, the special protection for children is justified by their lack of knowledge and understanding of consequences and legal rights, a concept called 'decisional vulnerability' which was defined by *Malgieri and Niklas.* In Rec.65 of GDPR, which highlights the issue of consent in the context of erasing personal data, the notion of children's decisional vulnerability is then reiterated. Likewise, Rec.58 demonstrates that the primary justification for protection is based on children's limited understanding. One can wonder, however, if any of the justifications for the protection of children in the framework for data protection can be taken into account - by analogy - also for other vulnerable individuals. The WP29 has also offered some guidance on this subject and noted in numerous views that vulnerability could not be restricted to only children, even if the solution is still unclear.[507]

According to WP29, the data on vulnerable data subjects should be taken into consideration when considering whether the processing is 'likely to result in a high risk' for the purposes of the GDPR. Due to the increasing power imbalance between the data subject and the data controller, processing of this sort of data may necessitate a DPIA because the data subject may not be able to give consent for or object to the processing of his or her data. Employees, for instance, frequently encounter significant challenges when attempting to challenge the processing carried out by their company, particularly when it relates to human resources management. Children can also be seen as lacking the capacity to consciously object to or provide their agreement to the processing of personal data. This also applies to

[506] Regulation (EU) 2016/679, OJL 119, Rec.38.
[507] Malgieri and Niklas, 'Vulnerable data subjects', 12.

highly at-risk groups of people who need extra protection, such as the elderly, those seeking refuge, people who are mentally ill, people who are patients, or in any situation where there is a clear power imbalance between the controller and the data subject.[508] The relationship between power imbalance and data subjects' vulnerability is evident in this situation. So, when the data controllers are in a position of significant power imbalance towards the data subject, particularly in terms of potential effects on fundamental rights and freedoms, significant information asymmetry based on predictive analytics, the latter should be regarded as vulnerable.

The WP29's Opinion on legitimate interests also aspires for a balanced approach that gives data controllers the required flexibility in circumstances where there is no undue impact on data subjects, while at the same time giving data subjects enough legal clarity and assurances that this flexible provision won't be abused. It is crucial to first take into account the nature and source of the legitimate interests, as well as whether the processing is required to further those interests, before weighing the impact on the data subjects. The relationship between the data controller and the data subject, including their balance of power, as well as whether the data subject is a child or otherwise falls into a more vulnerable population, must be taken into consideration when analysing the impact on the data subjects. While the average person should be used as the benchmark for the balancing test, specific circumstances should necessitate a more case-by-case approach. For instance, it would be relevant to take into account whether the data subject is a child or otherwise belongs to a more vulnerable population group that needs extra protection, such as the elderly, the mentally ill, or asylum seekers. The issue of whether the data subject is an employee, student, or patient, or if there is in any other way an imbalance between their position and the controller must unquestionably also be important. The impact of actual processing on particular people must be evaluated.[509] Once more, the concept of vulnerability is related to an imbalance of power.

In further Opinions, the WP29 stated that particular societal groups, such as vulnerable adults or minority groups, may be significantly impacted by processes that may have no

[508] Article 29 DPWP, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679', adopted on 4 April 2017, 17/EN/WP 248, 9.
[509] Article 29 DPWP, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC', adopted on 9 April 2014, 844/14/EN/WP 217, 41-50.

overall influence on individuals. For instance, a person in need of money who sees advertisements for online gambling frequently can take advantage of these offers and end up getting into further debt.[510]

It is worth noting that the GDPR emphasises the importance of risks to basic freedoms and rights. Particularly, under the GDPR's risk-based approach (Art.24), the data controller must put in place the necessary organisational and technical safeguards to ensure that the data protection principles are followed, by taking into account the nature, scope, context, and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. The controller should, of course, take into account scenarios in which a certain data processing could more severely harm some specific (vulnerable) individuals when assessing such risks of different likelihood and severity for rights and freedoms. According to Art.25 of GDPR, the controller should implement appropriate technical and organisational measures, such as pseudonymisation, both at the time of determining the means for processing and during the processing itself, to effectively implement data-protection principles, such as data minimisation, and to integrate the necessary safeguards into the processing to meet the requirements and protect the rights of data subjects. The data controller should consider the state of the art, the cost of implementation, the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons when applying for the data protection by design and by default principle.[511] Art.24 and Art.25 differ in that the data controller in the first situation just needs to demonstrate compliance with the data protection principles. He or she should 'apply' data-protection principles in the latter case in a manner that is reasonable given the state of the art and the implementation costs. It seems necessary in both situations to pay attention to vulnerable data subjects and to put in place specific measures to preserve their rights and freedoms.

The additional protection of vulnerable data subjects is provided by DPIA. Before processing, the controller should conduct an assessment of the impact of the proposed processing operations on personal data protection, where a type of processing, in particular using new technologies, and taking into account the nature, scope, context, and purposes of

[510] Article 29 DPWP, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679', adopted on 3 October 2017, 17/EN/WP 251, 11.
[511] Regulation (EU) 2016/679, OJL 119, Art. 24-25

the processing, is likely to result in a high risk to natural persons' rights and freedoms. As stated previously in Rec.75 and WP29, Art.35 also requires that a DPIA should be performed in cases of high-risk data processing, including cases where data subjects might be considered vulnerable. According to Art.35(7), the DPIA must at the very least include a systematic description of the processing, an assessment of need and proportionality, an assessment of risks, and a description of the measures planned to reduce those risks.[512] In other words, even if the accountability principle is followed, the data controller is responsible for the autonomous determination of measures to protect vulnerable persons. The DPIA can also resolve conflicts between the concept of vulnerability as a risk involved in the processing and the concept of vulnerability as a result of the processing of the data. The comprehensive approach of Art.35 necessitates a thorough analysis of risks, as well as a methodical description of the data processing and an evaluation of its necessity and proportionality. Additionally, the DPAs could issue explicit guidance on how to handle particularly vulnerable individuals through the use of the authority granted to them by Art.36.[513]

4.3.4. Summary

The GDPR is expected to bring a new rule and greater responsibility for large companies in the collection, recording, storage and general processing of data. Because otherwise, large companies will have cases of non-compliance, which will entail a very large number of fines for companies and which will not contribute to the economic turnover of companies. Putting privacy and personal data protection at the centre of processing, GDPR, in turn, would help better balances the roles of data subjects and data controllers. Since data subjects have processing rights vis-à-vis data controllers, the controller must also comply with its obligations vis-à-vis data subjects in a lawful, fair and transparent manner.

Since data protection law aims to protect the fundamental rights and freedoms of natural persons, and in particular their right to protection of personal data, it is clear that the position of natural persons as data subjects should be examined more thoroughly. Although data

[512] Ibid, Art. 35.
[513] Malgieri and Niklas, 'Vulnerable data subjects', 12.

subjects are identified and identifiable persons in the GDPR, it is worth defining some standard concepts of data subjects for further processing of personal data.

As a starting point in data protection law, it is advisable to introduce the average concept of the data subject as in consumer protection law, since in these two areas both consumers and data subjects are in a weaker position due to their status. Although the GDPR considers and applies the data processing rules to all data subjects without any distinction, it can be assumed from the reference to vulnerable natural persons, that on the contrary, there are non-vulnerable persons on whom the data controller can rely as average or standard data subjects in the data processing. The influential role of the data controller in the power imbalance of data processing information asymmetries also pushes for the definition of the status of average data subjects. All this leads to the need to introduce the standard concept of the average data subject in data processing for more effective functioning of the rights of data subjects in practice. By applying the concept of the average data subject in data protection law, it is possible to reduce the dependence of data subjects on information from data controllers in the processing of personal data.

In attempting to answer the research question of to what extent data protection law can provide an adequate definition of vulnerable data subjects, it is evident that the definition of vulnerable data subjects as an overall concept has not been fully developed. On the other side, the absence of average data subjects under data protection law may result in vulnerable data subjects being left in the shadow of general data subjects, with no additional protection. It follows that while the concept of vulnerability is evident in data protection law, it is still not effectively acknowledged as a foundation for identifying the social differences of data subjects. By introducing the concept of vulnerability into data protection law, especially concerning data subjects, it is possible to unlock the potential of the GDPR to protect the processing of personal data of various underprivileged data subjects.

The category of children as vulnerable data subjects is mentioned in the data processing with elements of consent and information obligations of data controllers. However, by analogy, data controllers cannot apply the same requirements in a different context to other categories of persons as vulnerable data subjects. Thus, more generally, it would be better if data controllers took special safety measures when processing the data of various categories of vulnerable data subjects. As the result, the data controller should also consider the

vulnerabilities of such data subjects when determining how to ensure that it complies with its transparency obligations concerning such data subjects if it is aware that their products or services are used by (or targeted at) other vulnerable members of society, such as people with disabilities or people who might have trouble accessing information.[514]

While data subjects as a term are unique and generic to all individuals, when interacting with data controllers, this can create some pros and cons for data controllers. Since data controllers are responsible for data processing, at any stage of processing, data controllers can exploit the vulnerabilities of data subjects without their knowledge, but for their own purposes. In addition, data controllers, being liable for the purpose and means of processing, must be mindful at every stage of processing of the nature, scope, and context of processing that could result in a high risk for data subjects' rights and freedoms. Thus, in general, when processing data, being responsible and accountable, the data controllers should avoid exploiting the vulnerabilities of data subjects for the sake of proper data processing. In all situations, data controllers should be aware of the implications of data processing for all categories of data subjects, especially vulnerable data subjects, and should, if necessary, consult DPI authorities in advance to mitigate the risks of processing.

[514] Article 29 DPWP, 'Guidelines on transparency under Regulation 2016/679', 17/EN WP260,10.

Chapter 5. E-commerce strategy and its regulatory mechanisms

The first part of this chapter focuses more on e-commerce security in general, with a focus on data processing security, network and communications security, and other new regulatory developments in the EU. And the emphasis will be on finding out to what extent existing security rules are sufficient to provide a proper environment for their users. The second part of the chapter assesses the current e-commerce strategy, especially the DSM Strategy. Later, the mechanisms for regulating areas related to e-commerce will be considered, especially given the latest digital transformation.

5.1. E-commerce security and its regulatory mechanisms in the EU

E-commerce is a force that cannot be stopped as the world's popularity rises quickly. When it comes to commercial operations, electronic technology is frequently employed to improve, expedite, and carry out expansion and augmentation, changing the way business was done. Modern information technology is important, but goods and services also have a big impact on how efficiently and effectively e-commerce works. However, due to the Internet's extensive e-commerce, doing business online will be faster but will raise significantly more security concerns. In the world of e-commerce, information security is a topic of widespread concern.[515]

The security of e-commerce transactions includes the security of the service's access, the participants' accurate identification and authentication, the exchanges' integrity, and, if necessary, their confidentiality. All of these safety precautions can go against what users expect in terms of transaction confidentiality and non-traceability.[516]

The security of Europeans includes cyber security. People should be able to use or visit linked gadgets, electrical grids, banks, aeroplanes, public administrations, and hospitals with the confidence that they will be protected from cyber dangers. More than ever, the economy, democracy, and society of the EU rely on trustworthy and safe digital tools and connectivity.

[515] Jianhong Li 'A Study on the Framework of the Security-Based E-commerce Applications' in Y.-H. Han et al. (eds.), *Ubiquitous Information Technologies and Applications: Lecture Notes in Electrical Engineering*, Dordrecht, Springer, vol.214, 2013, 639.
[516] Mostafa Hashem Sherif, *Protocols for Secure Electronic Commerce*, CRC Press, Boca Raton, 2016, 61.

As a result, security is crucial to creating a robust, environmentally friendly, and digital EU. The global, open Internet and network connectivity that are required to support the transformation of the economy and society in the 2020s also depend on security.[517]

Any security system can be defeated with adequate resources, according to the history of security in commercial transactions. Additionally, even in the information era, perfect protection of everything is not necessarily forever. Information has a time value, just like money does. A message can occasionally be protected for a few hours or days. Additionally, because security is expensive, it is always worthwhile to compare the price to any prospective gains. Last but not least, security is a chain that frequently fails at the weakest link. It can be settled that effective e-commerce security demands a collection of regulations, rules, policies, and technological advancements that, to the greatest extent possible, protect individuals and organisations from unforeseen conduct in the e-commerce market.[518]

However, the security of e-commerce systems is not a recent issue. The three fundamental security elements of e-commerce systems are confidentiality, integrity and availability, which also remain essential to computer and network security. An essential component of success in e-commerce is the security of its applications. Users must feel confident that the website is a legitimate company and will fulfil its obligations, that their credit card information is securely handled, and that their privacy is ensured before completing a transaction. Despite being inextricably linked to computer and network security, e-commerce security is different in many ways. First of all, e-commerce security needs are distinct from those of companies that do not have direct Internet access. Moreover, e-commerce security includes unique interaction protocols that demand extra security precautions. Finally, when it comes to individual or company assets, such as one's identity, confidentiality, credit card information, or direct Internet exposure, the risks are great.[519]

In today's digital economy, creating a secure e-commerce environment for companies is a crucial and difficult challenge. Utilising e-commerce technology is nearly impossible

[517] European Commission, 'Joint Communication to The European Parliament and The Council the EU's Cybersecurity Strategy for the Digital Decade, Brussels, 16.12.2020, JOIN (2020) 18 final, 1-4.
[518] Kenneth C. Laudon & Carol Guercio Traver, *E-commerce 2021–2022: Business, Technology, Society,* UK, Harlow, Pearson Education Limited, 2021, 296-297.
[519] Sviatoslav Braynov 'E-Commerce Vulnerabilities' in Hossein Bidgoli (ed) *Handbook of the Information Security: Threats, Vulnerabilities, Prevention, Detection, and Management,* vol.3, Hoboken, John Wiley & Sons, Inc., 2006, 68.

without completely secure online transactions. In addition, using this technology without safe e-commerce applications is very difficult to acquire the confidence of users. It is conceivable to link security problems to the Internet. The Internet's accessibility is the first factor. The global interchange of information is made possible by the free and open nature of the Internet. On the other hand, it provides a practical method for gathering and disseminating personal information. Additionally, security is also in danger due to the diversity of Internet users. Users cannot know which routers are involved in the distribution of online information; therefore, someone can reach the user information by scanning and tracking data.[520]

All participants in transactions are very concerned about the security of conducting e-commerce over the Internet. Information security is of utmost importance in today's online and interconnected world because a safe information infrastructure is essential to the success of e-commerce. Therefore, to handle the security of internet-based e-commerce effectively, the security issues must be addressed at the three levels. The initial level is the website's security which refers to the host computer's security. The next level is a service's security that covers the information of the distribution services' security. The last level is a transaction's security which refers to the need to protect transaction information from outsiders trying to access, understand, or tamper with it since it flew over the wire. E-commerce must be secured on four different fronts: a) the web clients, b) the data transaction, c) the web server, and d) the network server operating system. These four aspects of e-commerce must all be secure for the system to be functioning properly.[521]

Several security requirements must be met for e-commerce. The first requirement is authentication, which calls for the assurance of the parties' identities by the buyer, the seller, and the paying institutions. The next factor is integrity which is important for data and information sent in e-commerce, such as orders, responses to inquiries, and payment authorisations, which must be ensured to prevent unintentional or malicious alteration or destruction during transmission. Nonrepudiation is the third consideration. Merchants must be protected from the consumer's arbitrary refusal to place an order. Consumers, on the other hand, want protection against merchants that refuse to accept payments without good reason.

[520] Narmin Miriyeva, 'Security in Electronic Commerce and Online Payments' in MIRDEC-16th, International Academic Conference on Multidisciplinary Issues and Contemporary Discussions in Social Science, *Virtual/Online Conference Proceedings: Full Paper Series Rome 2020*, Mirdec & Globecos, Italy, 2020, 19.
[521] Bhasker, *Electronic commerce*, 202-270.

Then comes privacy which is a crucial consideration. Many clients demand the safety of their identity. They wish to keep their purchases hidden from others. Cash payments allow for ultimate privacy, which some people desire. Safety is the last component. Consumers want to know that giving their credit card information online is secure. Additionally, they need protection from fraud committed by merchants or by criminals acting as merchants.[522]

Security and privacy are strongly intertwined. Without security, privacy is impossible because any access that violates security measures is, by definition, illegal, unfair, and unlawful. Security generally protects against external bad actors, whereas privacy calls for procedures and mechanisms to safeguard data from such internal misuse. This is where privacy surpasses security. In that regard, privacy begins when maximum security has been put in place. According to one scholar, security is a necessary but insufficient condition for privacy.[523]

Information security, a crucial aspect of data protection, is a larger issue for all organisations. Although not all data is personal information, practically all of it has a value that the business has a stake in maintaining. The GDPR and other data protection laws are primarily concerned with safeguarding the rights of data subjects, but information security is also a necessary component of these laws and has much wider potential applications. Failures in data security and cyber breaches can be disastrous events for any corporation. Small businesses may be wiped out simply because of the nature of the breach or the immediate costs of dealing with it, while large corporations may face massive fines and class-action lawsuits, all of which can have serious ramifications and inflict significant damage on both the organisation's reputation and bottom line.[524]

5.1.1. Security of personal data

Today, data are a valuable resource for businesses and organisations. Organisations take considerable care to limit access to these data for both internal users within the company and external users outside the company since some of these data are worth millions of dollars.

[522] Turban et al., *Information Technology for Management*, 179.
[523] Nishant Bhajaria, *Data Privacy*, Manning Publications Co., Shelter Island, 2022, 45.
[524] IT Governance Privacy Team, 'EU General Data Protection Regulation (GDPR) An implementation and compliance guide', 113.

When dealing with concerns relating to the privacy of data on specific individuals, data security is equally essential; businesses and organisations managing such data must offer solid guarantees concerning the confidentiality of these data to adhere to legal requirements and policies. Overall, in the context of information system security, data security is crucial.[525]

Data security is distinct from a company's adherence to the privacy of its clients. Data security is a necessity for a business to defend the privacy of its users against outside dangers like malicious hackers. Contrarily, privacy refers to a company's obligation to shield its clients from the company's use of the data. Businesses usually concentrate on data security without realising that employees may access data in an intrusive manner. For instance, curious staff may examine the purchase history of a celebrity, which breaches the celebrity's privacy even if the celebrity's purchases are never reported in the media.[526]

Realising that most people effectively have two worlds one as a physical being and the other as a collection of digital data - is the first step in ensuring the security of personal information. It is crucial to understand that the majority of e-transactions entail the transfer of private digital data. People must be confident that these transactions are carried out securely. Additionally, it is essential to exercise caution while disclosing information because some identity thieves try to get sensitive personal data by impersonating reputable companies or organisations.[527]

The controller or processor should assess the risks involved in the processing and put measures in place to reduce those risks, such as encryption, to ensure security and prevent processing that violates GDPR. Given the current state of technology, the costs associated with implementation, the risks, and the character of the personal data that needs to be secured, those measures should ensure a suitable level of security, including confidentiality. The risks posed by processing personal data, such as accidental or unlawful loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed, which may in particular cause physical, material, or non-material damage, should be taken into account when assessing data security risk. Under Art.4(12) of GDPR, 'personal

[525] Ashish Kamra & Elisa Bertino 'Survey of Machine Learning Methods for Database Security' in J.J.P. Tsai & P.S. Yu (eds.), *Machine Learning in Cyber Trust: Security, Privacy, and Reliability*, New York, Springer Science + Business Media LLC., 2009, 54.
[526] Avi Goldfarb & Catherine Tucker, 'Why Managing Consumer Privacy Can Be an Opportunity', *MIT Sloan Management Review*, Special Collection: The Fine Line Between Service and Privacy, 2017, 1-3.
[527] Mitra Ananda, *Digital Security: Cyber Terror and Cyber Security*, New York, Chelsea House, 2010, 63-66.

data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.[528] It should be very clear what is meant by 'destruction' of personal data: this is when the data is gone or is gone in a form that is no longer useful to the controller. It should also be obvious by 'damage' it is meant that this is personal data that has been changed, corrupted, or is no longer complete. The phrase 'loss' of personal data should be understood to mean that although the data may still be there, the controller no longer has access to, control over, or possession of it. In addition, any additional processing that breaches the GDPR is considered unauthorised or unlawful processing, including the disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data. It ought to be obvious that a breach is a specific kind of security incident. The GDPR, however, only applies when there is a breach of personal data, as stated in Art.4(12). In summary, while all personal data breaches are security incidents, not all security incidents are automatically personal data breaches, and this underlines the distinction between a security incident and a personal data breach.[529] As a result, according to the security criteria, a personal data breach can be categorised as a) an 'availability breach' which refers to the unintentional or unlawful destruction or loss of personal data, b) an 'integrity breach' which refers to the alteration of personal data and c) a 'confidentiality breach' that means unauthorised disclosure of, or access to, personal data.[530]

The processing of personal data could result in physical, material, or non-material harms which could put the rights and freedoms of natural persons at risk, with varying degrees of likelihood and severity. Here are some particular situations such a) where the processing could result in discrimination, identity theft or fraud, financial loss, reputational damage, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymization, or any other significant disadvantage; b) situations in which data subjects could be denied their rights and freedoms or deterred from exercising control over their personal data; c) situations in which personal data are processed that reveal racial or ethnic origin, political opinions, religious beliefs, or philosophical beliefs, as well as membership in

[528] GDPR, Rec.83.
[529] Article 29 DPWP, Guidelines on Personal data breach notification under Regulation 2016/679', 7.
[530] Article 29 DPWP, 'Opinion 03/2014 on Personal Data Breach Notification', adopted on 25 March 2014, 693/14/EN WP 213, 4.

a trade union, the processing of genetic data, health data, or data pertaining to sex life, as well as criminal convictions and offences, or related security measures; d) in cases where evaluations of personal attributes are made, such as when analysing or forecasting characteristics relating to job performance, financial situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to develop or use personal profiles; e) where the processing of personal data relating to naturally vulnerable individuals, particularly children, occurs; or f) when processing impacts a high number of data subjects and uses a lot of personal data.[531]

All controllers and processors are subject to information and data security requirements under the data protection regime. It is necessary to adhere to these IT and personal data security rules. Even though internet use has increased data security threats, these problems are not just limited to an organisation's internet. The attention on security and data protection will grow as a result of the increasing number of data security breaches, including those caused by poor data security, internet use and social media, cloud computing, and online abuse.[532]

The controller and processor should implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation, the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The measures taken by the controller and processor include a) the pseudonymization and encryption of personal data; b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; c) the ability to restore the availability and access to personal data promptly in the event of a physical or technical incident; d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. The risks posed by processing, including those from accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed, must be assessed by considering the necessary level of security. Adherence to a recognised code of conduct as described in Art.40 or a recognised certification system as

[531] GDPR, Rec.75.
[532] Paul Lambert, *A User's Guide to Data Protection: Law and Policy*, UK, Bloomsbury Professional, 2020,155.

described in Art.42 may be used as a pattern of compliance with the standards outlined in Art.33, para.1 of GDPR. The controller and processor must take steps to ensure that any natural person acting under the direction of the controller or processor who has access to personal data does not process it except under the guidance of the controller unless he or she is required to do so under Union or MS law.[533]

If there is a breach of personal data, the controller must notify the supervisory authority (which refers to an independent public authority set up by a Member State following Art.51) responsible under Art.55 without undue delay and, if possible, no later than 72 hours after becoming aware of the breach. This is true unless the breach of personal data is unlikely to put the rights and freedoms of natural persons at risk. Under Art.55, on the territory of its own MS, each supervisory authority must be capable of carrying out the duties assigned to it and using the powers given to it under the GDPR. If the notification to the supervisory authority is not made within 72 hours, a justification for the delay must be included. When the processor finds a breach of personal data, they must notify the controller without undue delay. The notification must at least include the following information: a) a description of the nature of the personal data breach, including, if possible, the categories and approximate numbers of data subjects affected, as well as the categories and approximate numbers of personal data records involved; b) the name and contact information of the data protection officer or other contact points from which more information can be obtained; c) a depiction of the likely outcomes of the personal data breach; and d) a description of the actions by the controller has taken or intends to take to resolve the personal data breach, including, as necessary, steps to lessen any potential negative impacts.[534]

Under Art.34(1) of GDPR, the controller must communicate the data subject of a personal data breach without undue delay when the personal data breach poses significant harm to the rights and freedoms of natural people. The communication of the data subject referred to in para.1 of Art.34 should indicate in clear and straightforward language the nature of the personal data breach and should at a minimum comprise the information and measures referred to in Art.33(3) points (b), (c), and (d). Art.34(3) states that if any of the following circumstances are satisfied, the communication to the data subject referred to in para.1 of

[533] GDPR, Art. 32.
[534] Ibid, Art. 33.

Art.34 is not necessary. Here are some of these circumstances: a) The controller has put in place the necessary organisational and technical safeguards, and those safeguards have been applied to the personal information compromised. These safeguards should particularly include encryption technology that renders the personal information incomprehensible to anyone not authorised to access it; b) The controller has taken additional steps to make sure the high danger to the rights and freedoms of data subjects mentioned in Art.34, para.1 is no longer likely to occur; c) It would entail an excessive effort. In such a situation, public communication or similar action will be taken instead, informing the data subjects in an equally effective manner. If the controller has not already informed the data subject about the personal data breach, the supervisory authority may demand it to do so or may resolve that one or more of the circumstances outlined in Art.34, para.3, have been satisfied, taking into account the probability of a high risk of the personal data breach.[535]

5.1.2. Security of network and information systems

Every day, individuals and organisations use information. The utilised parts are frequently referred to as an information system. An information system (IS) is a collection of interconnected parts that gather, process, store, and distribute data and information as well as offer a feedback mechanism to achieve a goal. Increasing profitability or enhancing customer service are only two examples of how feedback mechanisms assist firms in achieving their objectives. Information has value in and of itself, and trading information for tangible objects is a common practice in commerce. Information is continually being created, stored, and transferred using computer-based systems. Financial institutions send billions of dollars electronically across borders, investors make multimillion-dollar choices of IS, and businesses acquire supplies and ship products more quickly than ever before. Businesses and our way of life will continue to evolve as a result of computers and ISs.[536]

The success of commercial transactions depends on the participants' confidence in each other's integrity, the value of the traded items, and the payment transfer and delivery mechanisms. Since most transactions involving e-commerce take place over distances, a

[535] Ibid, Art.34.
[536] Stair & Reynolds, *Fundamentals of Information Systems,* 4.

trusting environment needs to be created even if participants transact using dematerialised or even digital currencies. The security of the involved communication networks, including those that connect the seller and the customer, the participants with their banks, and the banks themselves, is essential.[537]

Our lives can be improved in a variety of ways by digital innovations like communications networks, AI, or quantum technology. But there are risks and expenses associated with using digital technologies. Citizens are increasingly overwhelmed by artificial attempts to get their attention and no longer feel in control of what happens to their personal data. Additionally, malicious cyber activity may endanger our personal safety, damage our vital infrastructure, and compromise broader security interests.[538]

Services and systems for networks and information are essential to civilization. Their dependability and security are crucial to societal and economic processes, particularly the internal market. The internet, in particular, network and IS, play a crucial part in facilitating the cross-border movement of commodities, services, and people. Due to their transnational nature, significant disruptions of those systems, whether planned or accidental, can have an impact on both the Union as a whole and specific MS, depending on where they happen. Therefore, for the internal market to operate as intended, the security of the network and information system are crucial. The Union's network and IS cannot be kept at a high degree of security with the current capabilities. The level of readiness among MS varies greatly, which has caused disparate strategies to be used throughout the Union. As a result, consumers and businesses are not protected to the same extent, and the Union's network and IS are less secure as a whole. It is consequently hard to establish a universal and successful framework for collaboration at the Union level due to the lack of standard requirements for operators of critical services and digital service providers. As a result, on July 6, 2016, the EU legislators adopted Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems (NISD) across the Union. This directive laid out measures to acquire a high common level of security of network and information within the Union to enhance the internal market's functionality. To accomplish this, the NISD a)

[537] Mostafa Hashem Sherif, *Protocols for Secure Electronic Commerce*, 61.
[538] European Commission, 'Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions: Shaping Europe's digital future', Brussels, 19.2.2020, COM (2020) 67 final, 1.

mandated that all MS adopt a national strategy on the security of network and IS; b) established a Cooperation Group to encourage and facilitate strategic cooperation, information sharing, and the growth of trust and confidence among MS; c) established a network for computer security incident response teams (the 'CSIRTs network') in a determination to foster mutual trust and confidence among the MS and quick and efficient operational collaboration; d) developed security and notification standards for digital service providers and operators of critical services; e) outlined requirements for MS to name single points of contact, CSIRTs, and national competent agencies to carry out activities connected to the security of networks and ISs. The actions taken by MS to protect their fundamental State interests, including those related to national security, including actions to protect information whose disclosure they deem to be incompatible with their security interests, and to uphold law and order, particularly to enable the investigation, detection, and prosecution of criminal offences, are unaffected by this Directive. Although the NISD referred to the processing of personal data following the DPD, the GDPR's requirements on data processing will apply since the DPD was repealed.[539]

Art.114 of the TFEU, whose goal is the establishment and operation of the internal market by improving measures for the approximation of national rules, serves as the legal foundation for the NISD. According to the CJEU's ruling in the *Vodafone and Others Case (C-58/08)*, the use of Art.114 TFEU is appropriate when there are discrepancies between national laws that have a direct impact on how the internal market operates. In addition, the Court ruled that where an act based on Art.114 TFEU has already eliminated all trade barriers in the area it harmonises, the Union legislature cannot be denied the ability to modify that act in response to any change in the situation or advancement in knowledge concerning its duty to protect the general interests recognised by the Treaty. Finally, the Court determined that the approximation measures covered by Art.114 TFEU are intended to leave room for discretion as to the approximation method most suitable to achieve the desired result, depending on the general context and the particular circumstances of the matter to be harmonised. By creating clear, generally applicable rules on the NISD's scope of application and harmonising the rules that apply to cybersecurity risk management and incident reporting,

[539] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJL 194, 19.7.2016, 1-30.

the proposed legal act would remove barriers and improve the establishment and functioning of the internal market for essential entities.[540]

The NISD is a major game changer for cybersecurity resilience and collaboration in Europe, as it was the first EU horizontal legislation to address cybersecurity concerns. The implementation of the NISD was therefore a crucial component of the cybersecurity package unveiled on September 13th, 2017, as it served as the foundation of the EU's response to the growing cyber threats and challenges that come along with the digitalisation of our economy and societal life. The Commission's 2016 Communication on Strengthening Europe's Cyber Resilience System has also acknowledged this view as a crucial point. MS should take the necessary steps to ensure that the provisions and cooperation models of the NISD can provide the best EU-level tools to achieve a high common level of security of network and ISs in light of the impending deadlines for the NISD's transposition into national legislation by 9 May 2018 and the identification of operators of essential services by 9 November 2018.[541]

'Network and information system' as used in the NISD means a) a network of e-communications falling under the purview of Art.2(a) of Directive 2002/21/EC; b) any device, group of interconnected devices, or set of related devices, at least one of which, following a program, automatically processes digital data; or c) digital data that is stored, processed, retrieved, or communicated by elements mentioned in points (a) and (b) to operate, use, protect, and maintain those elements. 'Security of network and information systems' refers to a network and information system's capacity to withstand, with a certain degree of confidence, any action that jeopardises the availability, authenticity, integrity or confidentiality of data that is stored, transmitted, or processed or the related services made available by or accessed through those networks and ISs. A framework containing strategic objectives and priorities on the security of network and ISs at the national level is referred to as a national strategy on the security of network and ISs. Each MS, to acquire and hold a high level of security of networks and ISs, should adopt a national strategy on the security of

[540] European Commission, 'Proposal for a Directive of The European Parliament and Of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148', Brussels, 16.12.2020, COM (2020) 823 final, 2020/0359 (COD), 3.

[541] European Commission, 'Communication from The Commission to The European Parliament and The Council Making the most of NIS - towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union', Brussels, 4.10.2017, COM (2017) 476 final/2, 2-6.

networks and ISs with the definition of strategic goals and measure rules. Each MS should appoint one or more national competent authorities (referred to as 'competent authorities') to oversee the security of networks and ISs at the very least for the industries and services listed in Annex II and III. MS may designate an existing authority or authorities to carry out this function. The national implementation of the NISD should be under the supervision of competent authorities. Each MS should establish a national single point of contact (the 'single point of contact') for network and information security. MS are free to appoint an existing authority to this position. When the MS names a single competent authority, that single point of contact is also that competent authority. The term 'digital service provider' means any legal person who offers a digital service, as opposed to 'operator of essential services,' which covers a public or private entity of the type mentioned in Annex II that satisfies the requirements stated in Art.5(2) of the NISD. The term 'digital service' refers to a service as defined in Art.1(1)(b) of Directive (EU) 2015/1535[542] that falls under one of the categories stated in Annex III of the NISD. MS should guarantee that operators of essential services and digital service providers take reasonable and proportional organisational and technical steps to manage the risks to the security of the networks and ISs they utilise. To guarantee the continuity of such services, MS should ensure that operators of essential services and digital service providers take the necessary precautions to prevent and mitigate the effects of incidents affecting the security of the network and ISs.[543]

5.1.3. Cybersecurity Act

Cybersecurity events seriously harm European businesses and the economy frequently. Such occurrences erode public and corporate confidence in the digital society. Each year, hundreds of billions of euros are lost due to the theft of commercial trade secrets, corporate information, and personal data, as well as the disruption of infrastructures and services, including vital ones. They may also have an impact on society as a whole and citizens'

[542] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification) (Text with EEA relevance), OJ L 241, 17.9.2015, 1–15.
[543] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJL 194, 19.7.2016, 1-30.

fundamental rights. The 2013 Cybersecurity Strategy of the EU and its key deliverable, the NISD, as well as Directive 2013/40/EU on attacks on information systems have served as the EU's primary policy responses to these cybersecurity challenges. Additionally, the EU has specialised organisations at its disposal including the Computer Emergency Response Team (CERT-EU), the European Cyber Crime Centre (EC3) within Europol, and the EU Agency for Network and Information Security Agency (ENISA). Despite these accomplishments, the EU is still susceptible to cyber incidents.[544]

When the disruption caused by a cybersecurity incident is too great for a concerned MS to handle on its own or when it affects two or more MS with such a broad impact of technical or political significance that it requires prompt coordination, and response and may be considered a crisis at the Union level. Any proper reaction must rely on both cyber and non-cyber mitigation strategies since cybersecurity crises have the potential to spark a larger crisis that affects sectors of activity outside networks, ISs and communication networks. The impacted parties and those responsible for responding to and minimising the effects of the incident must coordinate their reaction rapidly since cybersecurity incidents are unpredictable, frequently occur, and change over extremely short periods. Additionally, cyber catastrophes sometimes do not remain within a single country or region and might happen concurrently or spread quickly across several. Following the guiding principles outlined in the Blueprint Recommendation, MS and EU institutions should build an EU Cybersecurity Crisis Response Framework that incorporates the goals and modes of cooperation.[545]

Cybersecurity concerns are rising as a result of advanced connectivity and digitalisation, constructing society as completely more susceptible to cyber threats and escalating the risks faced by individuals, including children and other vulnerable people. There is a need for a comprehensive set of actions that would build on prior Union action and would encourage mutually reinforcing goals in light of the growing cybersecurity concerns the Union is facing. That is why with aim to reduce these risks, the EU legislators adopted Regulation (EU) 2019/881 of April 17, 2019, on ENISA and information and communications technology

[544] European Commission, 'Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry', Brussels, 5.7.2016, COM (2016) 410 final, 2.

[545] European Commission, 'Commission Recommendation (EU) 2017/1584 of 13 September 2017 on a coordinated response to large-scale cybersecurity incidents and crises', C/2017/6100, OJ L 239, 19.9.2017, 1.

cybersecurity certification, or shortly EU Cybersecurity Act (EUCA), which repeals Regulation (EU) No 526/2013. The EUCA aimed to create a high degree of cybersecurity, cyber resilience, and trust inside the Union while also assuring the correct operation of the internal market. The EUCA's scope is a) ENISA-related goals, duties, and organisational issues; and b) a framework for the creation of European cybersecurity certification schemes to guarantee a sufficient level of cybersecurity for ICT products, ICT services, and ICT processes within the Union as well as the aim of preventing the internal market from becoming fragmented concerning cybersecurity certification schemes within the Union. According to Art.2(1) of EUCA, 'cybersecurity' refers to the actions required to safeguard network and ISs, the users of those systems, and other individuals who may be impacted by cyber threats. Technology is simply one aspect of cybersecurity; human behaviour also plays a significant role. Therefore, 'cyber-hygiene,' which refers to easy, regular actions that citizens, organisations, and enterprises can take to reduce their exposure to dangers from cyberattacks, needs to be strongly encouraged. The ability of MS to fully respond to cyber threats, including cross-border incidents, must be maintained and expanded to improve the EU's cybersecurity infrastructure.[546]

Positive steps have already been made by EU law to recognise a new right to cybersecurity. If the language and strategies of the NISD and the EUCA are compared, clear progress in this direction can be seen. Although cautiously and minimally, the latter has made great progress in determining the fundamental elements of a new right, including the cybersecurity addressees and recipients, as well as its subject matter and extent. The definition of cybersecurity in the EUCA would read as follows if the prefix 'cyber' were simply removed then security means the activities necessary to protect assets, their users, and other persons from threats. Therefore, it would be acceptable to assume that cybersecurity is just real-world security projected into the digital sphere. Or, to put it another way, cybersecurity is a subset of security, assuring people that they will be just as secure online as they are

[546] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), PE/86/2018/REV/1, OJL 151, 7.6.2019, 15–69.

outside. In light of this, it follows that the basic right to security would suffice and that no new right to cybersecurity is required.[547]

5.1.4. The proposal and adoption of NIS2 Directive

Despite its remarkable successes, the NISD, which helped several MS adapt their institutional, regulatory, and mentalities toward cybersecurity, has now shown some of its shortcomings. The COVID-19 disease amplified society's digital transition, which has broadened the threat landscape and created new problems that call for creative and imaginative solutions. Cyberattacks are becoming more frequent, and they are getting more advanced as they come from both inside and outside the EU. The Impact Assessment highlighted the issues on how the NISD functioned such as the businesses operating in the EU having low levels of cyber resilience, variable resilience across MS, poor levels of shared situational awareness, and a lack of shared crisis management. Examples include situations where major hospitals in one MS did not fall under the NISD's scope and were therefore exempt from implementing the resulting security measures, whereas, in another MS, nearly every hospital in the country was subject to the NISD security requirements as a result of some of these issues and drivers.[548]

The EU's new Cybersecurity Strategy for the Digital Decade shapes an essential element of Shaping Europe's Digital Future[549], the Commission's Recovery Plan for Europe[550], the EU Security Union Strategy 2020–2025[551], the Global Strategy for the EU's

[547] Vagelis Papakonstantinou, 'Cybersecurity as praxis and as a state: The EU law path towards an acknowledgement of a new right to cybersecurity?' *Computer Law & Security Review*, vol.44, 2022, 105653, 7.
[548] European Commission, 'Commission Staff Working Document Executive Summary of The Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148', Brussels, 16.12.2020, SWD (2020) 344 final, 1.
[549] European Commission, 'Shaping Europe's digital future', COM (2020) 67 final, 1-16.
[550] European Commission, 'Commission Staff Working Document Identifying Europe's recovery needs Accompanying the document Communication from The Commission to The European Parliament, The European Council, The Council, The European Economic and Social Committee and The Committee of The Regions Europe's moment: Repair and Prepare for the Next Generation', Brussels, 27.5.2020, SWD (2020) 98 final, 1-54.
[551] European Commission, 'Communication from The Commission to The European Parliament, The European Council, The Council, The European Economic and Social Committee and The Committee of The Regions on the EU Security Union Strategy', Brussels, 24.7.2020, COM (2020) 605 final, 1-28.

Foreign and Security Policy[552], and the European Council Strategic Agenda 2019–2024[553]. It outlines how the EU will defend its citizens, companies, and institutions from online dangers, boost international cooperation, and take the lead in safeguarding a wide-open Internet.[554]

The EU Security Union Strategy emphasised that as the lines between the physical and digital worlds become increasingly hazy, security threats are relying more and more on interconnectivity and the ability to work across borders. Due by the end of 2020, the Commission was working on a proposal to replace the Directive on the identification and designation of European Critical Infrastructures (referred to as the 'ECI Directive') with a comprehensive cross-sectoral framework centred on non-cyber threats. This was done in conjunction with the NISD review. Overall, since the NISD's implementation, European nations have relied more and more on digital and information technologies, and their networks have connected more and more. The current ECI Directive covers infrastructures that would affect at least two MS in the energy and transportation sectors if they were to be disrupted. It was intended to achieve a stronger alignment between the NISD and the EU Critical Infrastructure Protection, particularly concerning the sectoral scope of both efforts. The EU Security Union Strategy for 2020 to 2025 also included provisions on cybersecurity, mentioning the review of the NISD that was anticipated to be finished by the end of 2020. Since the Commission has prioritised cybersecurity as part of its reaction to the COVID-19 situation, the Recovery Plan for Europe also includes increased expenditures in cybersecurity.[555]

The Commission made a proposal to replace the NISD to strengthen security requirements, address supply chain security, streamline reporting prerequisites, and submit more strict supervision measures and more stringent enforcement requirements, including

[552]European Union Global Strategy, 'A Global Strategy for the European Union's Foreign and Security Policy: 'Shared Vision, Common Action: A Stronger Europe,'' 2016, 1-60.

[553] European Council of the European Union, 'A new strategic agenda for the EU 2019-2024', <https://www.consilium.europa.eu/en/eu-strategic-agenda-2019-2024/> accessed 05 Aug. 2023.

[554] European Commission, 'the EU's Cybersecurity Strategy for the Digital Decade', JOIN (2020) 18 final, 1-29.

[555] European Commission, 'Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148', Brussels, 16.12.2020, SWD (2020) 345, final PART 1/3, 9.

harmonised sanctions across the EU, in response to the growing threats posed by digitalisation and the burst in cyberattacks.[556]

The proposal updated the current legal system to take into account recent increases in internal market digitisation and a changing landscape of cybersecurity threats. The proposal intended to lower compliance expenses for public and private organisations as well as the regulatory load placed on responsible authorities. This proposal was part of a larger package of current legal tools and impending Union-level actions aimed at improving the threat resiliency of both public and private entities. The provisions of the proposal at hand would replace the cybersecurity-related provisions of Directive (EU) 2018/1972 establishing the European Electronic Communications Code, and the proposal for a Regulation on digital operational resilience for the financial sector (COM (2020) 595 final) and would be regarded as '*lex specialis'* once both acts have entered into force. The proposal for a Directive on the resilience of critical entities, which amends Directive 2008/114/EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection (ECI Directive), is a complement to the proposal for physical security. The ECI Directive establishes a Union process for identifying and designating European Critical Infrastructures and lays out a strategy for improving their protection. The need for a more uniform and coherent approach between the ECI Directive and the NISD throughout the Union was highlighted.[557]

In the long run, the new proposed scope of NISD would help to increase the level of cybersecurity in Europe by effectively forcing more entities and spheres to take action. The new proposal would have three main goals in mind overall. The initial goal would be to raise the degree of cyber-resilience among a large group of companies operating in the EU across all pertinent industries. For instance, by including new industries like telecoms, social media platforms, and public administration, the proposal would greatly expand the horizons of the NISD. The next intention would be to lessen incompatibilities in resilience across the internal market in the spheres already touched by the directive by further harmonising the actual (de facto) scope, the requirements of the security and incident reporting, the national supervision

[556] EPRS/ European Parliamentary Research Service: EU Legislation in Progress briefing, 'The NIS2 Directive A high common level of cybersecurity in the EU', European Union, 2022, 1.
[557] European Commission, 'Proposal on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148', COM (2020) 823 final, 2020/0359 (COD), 1.

and enforcement of the ruling provisions, and the capacities of the relevant competent authorities of the MS. The proposal outlined a list of seven essential components, including incident response, supply chain security, encryption, and vulnerability disclosure, that all businesses must be addressed or implemented as part of the steps they took. The proposition also envisioned a two-stage incident reporting process. Affected businesses must file an initial report within 24 hours of learning about an incident, followed by a final report no later than one month after the initial report. The final intent would be to raise trust between responsible authorities, share more information, and establish norms and procedures in the case of a major incident or crisis by boosting joint situational awareness and collective competence. By adopting clear responsibilities, sufficient planning, and more EU interaction, the proposed new rules would enhance how the EU precludes, manages, and reacts to significant cybersecurity incidents and crises.[558]

Based on this proposal, on December 14, 2022, the EU legislators adopted Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union or shortly known as NIS2D, by amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148. The NIS2D outlines actions that are intended to create a high degree of cybersecurity that is shared throughout the Union in order to enhance the internal market's functionality. The NIS2D aims to establish the following obligations: a) MS are obligated to adopt national cybersecurity strategies and identify or set up competent authorities, cyber crisis management authorities, single points of contact on cybersecurity, and CSIRTs; b) cybersecurity risk-management procedures and reporting requirements for organisations of the kinds mentioned in Annex I or II as well as for organisations designated as critical entities under Directive (EU) 2022/2557; c) guidelines and requirements for sharing cybersecurity information; and d) requirements on MS in terms of supervision and enforcement. The NIS2D is applicable to public or private organisations of the kinds listed in Annex I or II that fall under the definition of a 'medium-sized enterprise' as defined by Art.2 of the Annex to Recommendation 2003/361/EC or that exceed the limits for such enterprises set forth in paragraph 1 of that Article and that perform their services or engage in their business operations within the Union. Regardless of their size, entities recognised as critical enterprises under Directive (EU) 2022/2557 and entities offering

[558] EPRS, 'The NIS2 Directive A high common level of cybersecurity in the EU', 7.

domain name registration services are subject to the NIS2D. The NIS2D does not affect the Member State's obligation to protect national security or its authority to protect other crucial state responsibilities, such as preserving the State's territorial integrity and upholding peace and order. Public administration organisations that carry out their operations in the fields of national security, public security, defence, or law enforcement, including the prevention, investigation, detection, and prosecution of criminal acts, are exempt from the NIS2D. If MS implement or maintain measures to provide a greater level of cybersecurity, the NIS2D shouldn't prevent them from doing so as long as they comply with the duties set down in Union law. MS should adopt and publish the measures necessary to comply with the NIS2D by October 17, 2024, and should promptly notify the Commission of such adoption or publication. The MS should implement such provisions by October 18, 2024, the same day that Directive (EU) 2016/1148 is repealed.[559]

5.1.5. Summary

E-commerce security is an essential component of the efficient and reliable operation of e-commerce systems and their participants. Users should be careful about information being disclosed when making online transactions. The businesses must also make sure that the proper organisational and technical safeguards are in place to guarantee a degree of security proportional to risk. When it comes to the security of personal data, greater responsibility and accountability falls on the data controllers and how they fulfil their data obligations towards other participants. Data breaches that pose a risk to individuals' rights or freedoms should be reported to supervisory authorities and communicated to data subjects without excessive delay.

The rise in cyber-attacks and poor cyber resilience across the Union demonstrated that the cybersecurity sector needed to be revised to achieve common national implementation. Given that the NISD was too limited in the areas of security, lacked sufficient clarity in the operations of service providers, and had ineffective monitoring and enforcement, it is not

[559] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance), PE/32/2022/REV/2, OJ L 333, 27.12.2022, 80–152.

surprising that the revision of the NISD was one of the main goals of cybersecurity policymakers in the EU. The EU will increase cyber resilience, create reporting duties, and eliminate unequal cybersecurity implementation across the MS with the new NIS2D. Whether the new cyber security measures will be sufficient to provide an effective environment for cyber resilience and remove barriers to national fragmentation will only be known after the implementation of the NIS2D rules. However, within the framework of the EU Security Union Strategy and the Cybersecurity Strategy for the Digital Decade, great and successful results can be achieved with the effective cooperation of the relevant authorities in the MS and a minimum set of regulatory rules.

Trying to answer the research questions about the extent to which the EU is able to regulate security issues in e-commerce, it can be seen that at the moment there will be a review and transformation of the rules based on the latest technological developments, keeping in mind the interests of users and the requirements of society. Given that digital transformation and other unforeseen circumstances (in particular Covid-19) make people and businesses more dependent on networks and communication systems, this also brings up new security issues and challenges. As the EU security sector is in the middle of a revision phase, it is expected that there will also be a period of experimentation, errors, and speculations with the application of the rules of the NIS2D in practice. Unfortunately, despite the efforts of practitioners and policymakers to learn about all the failures and successfully implemented measures from the previously applied NIS Directive, the results show that they were not as sufficient and effective as expected. So, it is reasonable to assume that with the cooperation and coordination of the relevant authorities, businesses and individuals will feel safer and more secure from any cyberattacks and invasions, with the new NIS2D offering some optimism for the future.

5.2. E-commerce strategy and its regulation

It is commonly known that there is a digital transformation happening. Digital transformation is being shaped by many distinct factors. A genuine digital transformation must begin with European businesses and citizens having trust in the security of their products and applications. However, for this digital transformation to be fully successful, it will need

to establish the proper frameworks to guarantee reliable technology and to provide businesses with the assurance, expertise, and resources they need to go digital. To do this and strengthen European digital leadership, coordination of activities between the EU, MS, regions, civil society, and the commercial sector is essential.[560]

The core of the founding fathers' vision for Europe was the creation of a single, massive market. They were aware of the value of cooperating, trading and organising to build a world that was richer, more inventive, clever, fair, and stronger. That was, and still is, the goal of the large European market: sharing a common economic and social space while respecting diversity, the desire to come together and strengthened by the wisdom of standing together. The names of the large European market have changed throughout time to represent the simultaneous phenomena of its expansion and diversification: Common Market, Internal Market, and Single Market (SM). The four major freedoms of movement of people, goods, services, and capital were further developed, but the economic integration that was being strengthened, the emergence of a common currency, and the advancement of the cohesion policy were all added to and enhanced this process.[561]

5.2.1. The Single Market of the EU

Since its inception, the Common Market, which is now known as the Internal Market, has been at the centre of the European project. For more than 50 years, it has woven strands of solidarity between men and women in Europe while also creating new opportunities for growth for more than 21 million European businesses. Since 1993, the Euro, economic integration, and solidarity and cohesion policies have strengthened the Internal Market, a region of free movement for commodities, people, services, and capital. A proactive and comprehensive strategy should be created to address these issues and allow the SM to reach its full potential. The Commission presented for discussion 50 measures in the Communication 'Towards a Single Market Act' to address these issues. The Single Market

[560] European Commission, 'Shaping Europe's digital future', COM (2020) 67 final, 5-15.
[561] European Commission, 'Communication from The Commission to The European Parliament, The Council, The Economic and Social Committee and The Committee of The Regions Towards a Single Market Act: For a highly competitive social market economy: 50 proposals for improving our work, business and exchanges with one another', Brussels, 27.10.2010, COM (2010) 608 final, 2.

Act was generally backed by the Council in its Conclusions of December 10, 2010, giving it a strong economic and social foundation in a highly competitive economy. To stimulate growth and boost citizens' confidence, the Commission determined twelve levers on April 6, 2011, based on comments made during the public debate. The Action Plan was merely the first step in that direction, even while it satisfied the urgent need to take action for growth and jobs.[562]

The Single Market, also known as the Internal Market, allows people, services, products, and capital to flow more freely between the EU MS, creating opportunities for both businesses and consumers. It is one of the EU's major successes and the foundation of economic integration inside the EU. The 'four freedoms' relate to the free movement of goods, people, services, and capital from one EU Member State to another. The SM is not limited to only the EU MS; Iceland, Norway, and Liechtenstein also participate through the European Economic Area Agreement (EEA). The following guiding principles shape the foundation of the SM: mutual recognition, free movement, subsidiarity, and proportionality. The latter two regulate the application of EU policies in areas that are not solely within its competence, such as the SM. A broad premise of EU law that also applies to the SM is the prohibition against discrimination. Certain aspects of the SM are governed by harmonised laws at the EU level, others are subject to national regulation.[563]

Articles 4(2)(a), 26, 27, 114, and 115 of the TFEU provide the legal foundation for the SM. Particularly, under Art.114 of the TFEU, the EU parliament can adopt measures for the approximation of laws in the MS with the goal of establishing and operating the SM. The approximation is designed to meet the goal of Art.26, which is to establish or assure the functioning of the SM, by ensuring harmonised legislation across the EU and limiting regulatory discrepancies between MS.[564]

The SM's expansion is a never-ending process. The SM must adapt to a world that is continually evolving, where the strain on natural resources, climate change, social and

[562] European Commission, 'Communication from The Commission to The European Parliament, The Council, The Economic and Social Committee and The Committee of The Regions Single Market Act: Twelve levers to boost growth and strengthen confidence 'Working together to create new growth'', Brussels, 13.4.2011 COM (2011) 206 final, 2-4.
[563] E. Dahlberg, et al., 'Legal obstacles in Member States to Single Market rules', Publication for the committee on Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2020, 21.
[564] TFEU, Art.114.

demographic difficulties, and new technology and imperatives must all be taken into account. As a fundamental tool for achieving the long-term goal of a vibrant, social market economy, the SM increases Europe's ability to compete in the world market.[565] The European Commission has made it a priority to give consumers legal access to goods and services from throughout the SM.[566]

In recognition of the significance of strengthening and deepening the SM, the European Commission outlined a strategy in its 2012 Communication on better governance for the SM with the following objectives: a) concentrate the efforts of the Commission and the MS on a small number of areas, particularly on the service sectors and the network industries and take the necessary measures to ensure that the SM's full potential in these areas can be realised; b) guarantee that Directives in these areas are quickly transposed, effectively applied, and enforced; and c) observe and specify remedial action(s) in the European semester process.[567]

The SM is not a goal unto itself, as well. It served as a tool for carrying out other policies. If the SM functions as it should, all public and private initiatives, as well as solutions to the problems of growth, social cohesion, employment, security, and climate change, would have a greater chance of success. The EU 2020 strategy, which included seven flagship initiatives, must therefore include the relaunch of the SM. These initiatives were: a) an innovation union; b) youth on the move; c) a digital agenda for Europe; d) resource-efficient EU; e) an industrial policy for the globalisation era; f) an agenda for new skills and jobs; and g) a European platform to combat poverty.[568]

There is no doubt that additional efforts will be required in the future to keep the SM operating as a growth and welfare engine as the current crisis develops and new problems appear. Because of this, Communication declared in 2012 that 'Single Market Act II' included a new set of priority actions. These steps were intended to produce tangible results on the

[565] European Commission, Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions Single Market Act II Together for new growth (Text with EEA relevance), Brussels, 3.10.2012, COM (2012) 573 final, 4.
[566] Patrice Muller et al., European Added Value Assessment, Better Governance of the Single Market, An assessment accompanying the European Parliament's Legislative own-Initiative Report, EAVA 2/2013, Brussels, European Union, 2012. 24.
[567] European Commission, 'Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions Better Governance for The Single Market', Brussels, 8.6.2012, COM (2012) 259 final, 8-9.
[568] European Commission, 'For a highly competitive social market economy: 50 proposals for improving our work, business and exchanges with one another', COM (2010) 608 final, 4.

ground and gave citizens and companies the confidence to take advantage of the SM. Importantly, it would take ongoing political support from all actors for the vision of the SM to become a reality for citizens and businesses. The first Single Market Act already benefited from the Commission, European Parliament, and Council working together collaboratively. For the Single Market Act II to be delivered, the same collaborative spirit would be necessary.[569]

According to the European Commission 2013 Annual Growth Survey, the European SM offered many opportunities for businesses to develop and for consumers to benefit from better services and products. Improved Services Directive implementation, enhanced network industry performance, adoption of European-level standards, and notification of technical rules for ICT products and services to facilitate their circulation in the SM were among the priority areas that were singled out for action.[570] Typically, the SM initiatives involved either a Directive that must be adopted and enforced by MS or a Regulation that must be transferred into national law.[571]

Therefore, the SM needed to be revitalised and modernised in a way that enhanced the performance of the markets for goods and services and ensured that people are given the necessary protection. That was what the strategy attempted to do and it consisted of focused actions in three key areas: a) providing opportunities for consumers, professionals, and businesses; b) fostering and facilitating the modernisation and innovation that Europe needed; and c) making sure that the implementation was doable and beneficial to consumers and businesses in their day-to-day operations.[572]

The Internal Market must continuously adjust to the rapidly evolving conditions brought on by the digital revolution and globalisation. New chances for organisations and individuals are being created by the new era of digital innovation, which also generates new opportunities for the effective creation of high-quality data. It poses an equal threat to safety, consumer protection, enforcement of laws, and regulation. Before now, there have been

[569] European Commission, 'Single Market Act II Together for new growth', COM (2012) 573 final, 5.
[570] European Commission, 'Communication from The Commission: Annual Growth Survey 2013', Brussels, 28.11.2012, COM (2012), 750 final, 8.
[571] Muller et al., 'European Added Value Assessment, Better Governance of the Single Market', 13.
[572] European Commission, 'Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions Upgrading the Single Market: more opportunities for people and business', Brussels, 28.10.2015, COM (2015) 550 final, 3.

separate programmes for Union action in the areas of financial services policymaking, consumer protection, customers and end-users in the financial services industry, and plant, animal, food and feed. A few extra initiatives have received direct funding from the Internal Market budget streams. To finance initiatives aimed at creating a functional, sustainable Internal Market, it is now required to streamline and capitalise on synergies between diverse actions. Additionally, a more flexible, transparent, straightforward, and adaptable framework must be provided. Therefore, a new programme should be created that combines initiatives previously funded under those other programmes with other pertinent budget lines. Along with existing initiatives, that programme ought to incorporate fresh ones that seek to enhance the Internal Market's functionality without duplicating efforts with related EU initiatives. As a result, on April 8, 2021, the EU legislators implemented Regulation (EU) 2021/690 on establishing a programme for the internal market, competitiveness of enterprises, including SMEs, the area of plants, animals, food, and feed, and European statistics or shortly known as Single Market Programme. The Program's duration corresponded to that of the multiannual financial framework. Overall, this Regulation establishes a programme to enhance the efficiency of the internal market, the competitiveness and sustainability of businesses, particularly micro, small, and medium-sized businesses, and consumer protection, to manage spending on plants, animals, food, and feed, and to establish the programming and financing framework for the development, production, and dissemination of European statistics within the meaning of Art.13 of Regulation (EC) No 223/2009 (Single Market Programme) (the 'Programme') for the period from 1 January 2021 to 31 December 2027. The objectives of the Programme and the eligible activities for achieving those objectives are also outlined in this Regulation, together with the budget for the years 2021 to 2027, the types of funds the Union will provide and the guidelines for doing so, and the program's governance structure.[573]

5.2.2. The Digital Single Market and its Strategy

[573] Regulation (EU) 2021/690 of The European Parliament and Of The Council of 28 April 2021 establishing a programme for the internal market, competitiveness of enterprises, including small and medium-sized enterprises, the area of plants, animals, food and feed, and European statistics (Single Market Programme) and repealing Regulations (EU) No 99/2013, (EU) No 1287/2013, (EU) No 254/2014 and (EU) No 652/2014 (Text with EEA relevance), PE/18/2021/INIT, OJ L 153, 3.5.2021, 1–47.

The balance of societal and economic interactions has been drastically altered by digital technology, creating new possibilities for creative business models. In practice, the EU is dedicated to modernising the SM for the digital era. One of the ten objectives of the European Commission, which intends to respond effectively to the difficulties of the digital revolution to take advantage of this opportunity for economic growth, is the implementation of a connected DSM. This extensive political plan contains many different components. To improve consumer and data subject protection, as well as give businesses the legal security they need to make investments in this area and foster growth and innovation, a comprehensive and well-organized set of standards is necessary.[574]

A DSM is one in which, regardless of nationality or place of residence, the free movement of goods, people, services, and capital is guaranteed. Additionally, citizens, individuals, and businesses can easily access and engage in online activities under the conditions of fair competition and a high level of consumer and personal data protection. Achieving a DSM will help European businesses expand internationally and ensure that Europe keeps its position as a worldwide leader in the digital economy. A fully operational DSM will provide European businesses, especially SMEs with a potential client base of over 500 million people, allowing them to fully utilise ICT to scale up for productivity improvements while simultaneously producing growth.[575]

The DSM Strategy was introduced by the EU Commission on May 6, 2015, and it benefited from input and discussion with the MS, the European Parliament, and stakeholders. Its multiannual scope and significant interdependent initiatives - which can only be carried out at the EU level - are its main focal points. These points have been selected to have the greatest possible impact, can be carried out during the current Commission's term, and will be advanced following better regulation principles. Every action will be the subject of proper consultation and impact evaluation. Three pillars would back up the DSM Strategy. The initial one is improved consumer and business access to digital products and services throughout Europe. To remove obstacles to cross-border online activities, significant discrepancies

[574] Alberto De Franceschi (ed) *European Contract Law and the Digital Single Market.* The Implications of the Digital Revolution: Current Issues and New Perspectives', Cambridge, Intersentia Ltd, 2016, 1-17.
[575] European Commission, 'Commission Staff Working Document: A Digital Single Market Strategy for Europe - Analysis and Evidence Accompanying the document, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Single Market Strategy for Europe', Brussels, 6.5.2015, SWD (2015), 100 final, 1.

between the online and offline worlds must be quickly eliminated. The next pillar is establishing favourable conditions for the development of digital networks and services. This demands infrastructures and content services that are fast, secure, and reliable, supported by the proper legal frameworks for innovation, investment, fair competition, and level playing fields. The last one is exposing the development potential of the European Digital Economy. To increase industrial competitiveness and improve public services, inclusivity, and skills, it is necessary to invest in ICT infrastructures and technologies like Cloud computing and Big Data.[576]

The DSM Strategy seeks to strengthen the EU in many ways, all of which relate to the promotion of a DSM. It offers a lot of crucial milestones along the route, but more work needs to be done. The majority, but not all, of the DSM Strategy's advantages stem from either: a) advancing the SM in the digital sphere, or b) advancing the EU's digitalisation. The electronic ordering of both real and virtual products and services would be as simple and affordable on a cross-border level as it is on a local one in a truly DSM. The establishment of a business and many other e-government services, such as health care, would be just as simple and affordable internationally as they are domestically. Lower pricing, more options and convenience for consumers, scale economies, and increased competitiveness of the EU concerning its international trading counterparts could all be anticipated as a result of the SM benefits. Digital technology would be utilised far more in a truly DSM than it is in the EU today. The EU's economy and society are set to undergo radical change as a result of fast broadband, mobile (5G) services, AI, robots, big data, machine learning, the Internet of Things (IoT), cloud computing, and blockchain. It is anticipated that the EU will become fully digitalised, leading to increased productivity, decreased transaction costs, new product, service, and process innovation, and improved EU competitiveness in contrast to the EU's international trade partners. In conclusion, the benefits of the legislation under the DSM Strategy stem from two independent dimensions: gains from the SM and gains from digitalisation. However, there is not a total overlap of benefits in either dimension.[577]

[576] European Commission, 'A Digital Single Market Strategy for Europe', COM (2015) 192 final, 3.
[577] Alexendre de Streel et al., 'Contribution to growth: The European Digital Single Market, Delivering economic benefits to citizens and businesses', Study for the Committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2019, 11.

By removing obstacles to cross-border e-commerce and access to online content, the DSM intends to create a cohesive digital market where companies and individuals may buy and sell products and services and operate freely and seamlessly. The DSM is significant because it may stimulate innovation, increase competition, produce significant economic growth, and improve consumer welfare and choice. At a particular point when market and government services are quickly transitioning from fixed to mobile platforms and becoming more commonplace, the DSM increases the economy, reduces environmental consequences, and improves the quality of life. The DSM can spur innovation and economic growth by expanding and integrating the market for digital goods and services. This will raise demand and bring about economies of scale, which will encourage more investment in digital infrastructure, technology, and R&D. Additionally, removing obstacles to international trade and investment can increase competition and encourage the development of new business models and services. The DSM can also offer citizens advantages in terms of data protection, privacy, and digital security by standardising laws and norms across the EU. This not only protects citizens' rights but also boosts confidence in e-commerce and online transactions across the EU.[578]

President von der Leyen stated that Europe should guarantee digital sovereignty with a shared vision of the EU in 2030, based on clear aims and principles, in the State of the Union Address in September 2020. In response, the European Council requested that the Commission provide a thorough Digital Compass by March 2021, describing digital ambitions for 2030, establishing a monitoring system, outlining significant milestones, and outlining how these ambitions will be achieved. To expedite Europe's digital transformation, the work started over the decade prior needs to be intensified. This means building on the DSM's progress and stepping up the initiatives outlined in the plan for Shaping Europe's Digital Future. A programme of policy reform was outlined in the strategy, and it has already begun with the passage of the Data Governance Act, the Digital Services Act, the Digital Markets Act, and the Cybersecurity Strategy.[579] Then this proposal led to the adoption of

[578] David Ashton et al., 'EU Mapping: Overview of Internal Market and Consumer Protection related legislation, publication for the Committee on Internal Market and Consumer Protection', Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, European Union, 2023, 22.
[579] European Commission, 'Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions 2030 Digital Compass: the European way for the Digital Decade', Brussels, 9.3.2021, COM (2021) 118 final, 1-2.

Decision (EU) 2022/2481 on establishing the Digital Decade Policy Programme 2030 on 14 December 2022 to encourage innovation and investment in the EU. The digital goals for 2030 are based on four pillars: digital skills, digital infrastructures, digitalisation of business and public services.[580]

Later the Regulation (EU) 2021/694 on establishing the Digital Europe Programme in April 2021 was passed with the objectives: a) to strengthen and promote Europe's capacities in key digital technology areas through large-scale deployment; and b) in the private sector and areas of public interest, to widen the diffusion and uptake of Europe's key digital technologies, promoting the digital transformation and access to digital technologies. The program's overall goals should be to support and accelerate Europe's economic, industrial, and social transformation towards a digital economy, to benefit its citizens, public administrations, and businesses across the Union, and to increase Europe's competitiveness in the global digital economy, through comprehensive, cross-sectoral, and cross-border support as well as a stronger Union contribution. It also could help close the digital divide in the Union and strengthen its strategic autonomy.[581]

The moment has come for the EU to specify how its principles and fundamental rights should be applied in the online world in light of the speeding up of digital transformation. Later, intending to promote a European attitude towards people-centred digital transformation, on January 26, 2022, the Commission published a Declaration on Digital Rights and Principles for a Digital Decade, which is based on the ideals of the EU and benefits everyone.[582] This Declaration is a response to the European Parliament's calls for full adherence to fundamental rights, including data protection laws and equal treatment, inclusiveness, and principles like technological and net neutrality, as well as for the development of high-performing digital education ecosystems. It also considers the

[580] Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (Text with EEA relevance), PE/50/2022/REV/1, OJL 323, 19.12.2022, 4–26.
[581] Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (Text with EEA relevance), PE/13/2021/INIT, OJ L 166, 11.5.2021, 1–34.
[582] European Commission, European Declaration on Digital Rights and Principles for the Digital Decade Brussels, 26.1.2022, COM (2022) 28 final, 1.

Parliament's request to safeguard media freedom, combat misinformation, and protect users' rights in the digital environment.[583]

5.2.3. The current regulatory mechanisms of the e-commerce-related areas

The establishment of an information society service providers, or e-commerce providers, and their immunity from responsibility are covered in ECD 2000/31/EC, often known as the Mother Directive or Framework Directive.[584] It provided uniform guidelines for the EU on a range of e-commerce-related topics, including online services, advertising, spam, online contracts, enforcing existing laws, and service providers' liability. Since the e-commerce field is considered to be a comprehensive and multidisciplinary industry, it is not surprising that it also encompasses other related areas such as consumer protection, data protection, privacy and online security, online digital markets and online intermediary services. In the previous chapters, most of the above-mentioned areas have been examined from the EU regulatory perspective, which is why the focus here is on the recent digital transformation of society and the economy.

The ECD's goal is not to harmonise criminal law per se, but rather to establish a legal framework to allow the open distribution of information society services between MS. Insofar as the ECD does not restrict the freedom to provide information society services, it supplements Community law applicable to information society services without compromising the level of protection for, in particular, public health and consumer interests, as established by Community acts and national legislation implementing them. The ECD neither seeks to establish tax regulations nor does it foreclose the creation of any Community instruments addressing the tax implications of e-commerce. The ECD does not apply to a) the area of taxation; b) matters relating to information society services covered by Directives 95/46/EC and 97/66/EC; c) matters relating to agreements or practices governed by cartel law, and d) the following activities of information society services, in particular the activities

[583] European Commission, 'Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions Establishing a European Declaration on Digital rights and principles for the Digital Decade', Brussels, 26.1.2022, COM (2022) 27 final,1.
[584] Arno R. Lodder 'The European Union and e-commerce' in Arno R. Lodder and Andrew D. Murray (eds), *EU Regulation of E-Commerce: A Commentary*, Cheltenham, Edward Elgar Publishing Limited, 2017, 11.

of notaries or equivalent professions, insofar as they imply a direct and specific connection with the exercise of public authority, representation of the client and protection of his interests in courts and gambling activities related to betting with a cash equivalent in gambling, including lotteries and totalizators.[585]

E-commerce's importance to the EU cannot be overstated. In the past, converting trade to e-commerce allowed technology to be used to enhance the EU economy. The ECD enabled e-commerce to grow throughout the EU MS by establishing a legal framework for information society services without internal borders, which was appropriate at the time of its inception. This helped to launch the development of the DSM. By practically removing the distance between European traders and consumers, the ECD enabled the development of economic ties among EU members despite geographical barriers. The ECD was built upon the already existing Community acts and was seen as a keystone for a fully functional Internal Market. The ECD was designed to promote economic growth, for example, by encouraging new employment opportunities and boosting European industry's competitiveness. The liability rule for technological intermediaries was one area where the ECD has been challenged for having protection gaps that leave basic human rights unprotected. In addition, as shown by numerous subsequent studies, this Directive has proven to be a tremendous first success in achieving the goals for which it was finalised, particularly establishing an acceptable legal framework for information society services and decreasing legal uncertainty.[586]

It was not enough to simply remove State barriers between MS to exploit the full potential of the internal market, which was a region devoid of internal borders where, among other things, the free movement of goods and services was guaranteed. Private parties may raise barriers that were incompatible with the freedoms enjoyed by the internal market, undermining such removal. This happened when businesses based in one Member State restricted or banned clients from other MS who want to conduct cross-border business from using their online interfaces, such as websites and applications. This phenomenon was known as geo-blocking. As a result, Regulation (EU) 2018/302, a component of the DSM, aimed to support the proper operation of the internal market by forbidding unjustified geo-blocking

[585] Directive 2000/31/, OJ L 178, 1–16.
[586] Hans Schulte-Nölke et al., 'The legal framework for e-commerce in the Internal Market', Study for the committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2020, 14-15.

and other types of discrimination based on the customer's nationality, place of residence, or place of establishment, directly or indirectly.[587]

Over the past years, there has been a significant shift in how businesses and customers pay for goods and services. These changes are being fuelled by the rapid expansion of e-commerce, and new payment systems are being created to support online purchases. More recently, the proliferation of the internet has stimulated the creation and adoption of fresh, inventive payment solutions, even for traditional payment scenarios like those at the point of sale.[588] Since the adoption of Directive 2007/64/EC (PSD) and the subsequent consideration of recent developments in e-payments, Directive (EU) 2015/2366 on payment services in the internal market, often referred to as the Payment Services Directive 2 (PSD2) was adopted by EU legislators. The PSD2 focused on rules establishing the transparency of payment service terms and the respective rights and obligations of payment service users in the internal market.[589] Later as one of the positive changes that occurred was the launch of the European Payment Initiative (EPI) project on July 2, 2020, by a group of 16 European banks, intending to create a pan-European payment system by 2022. Parallel to this, numerous initiatives spearheaded by the European Payments Council (EPC) and the Euro Retail Payments Board (ERPB) worked to create standardised European norms and schemes to promote the emergence and interoperability of instant payment solutions in brick-and-mortar as well as e-commerce.[590]

5.2.3.1. New regulatory proposals for the transformation of digital sectors

Digital technologies have had a profound impact on every aspect of daily life and the economy over the past ten years. Data is at the epicentre of this transition, and data-driven

[587] Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC (Text with EEA relevance.) OJ L 60I, 2.3.2018, 1–15.
[588] Narmin Miriyeva 'European Payments in the Digital Age', *ELTE Law Journal*, Eötvös University Press, 2022/2, 45.
[589] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), OJL 337, 23.12.2015, 35–127
[590] Miriyeva 'European Payments in the Digital Age', 48.

innovation will greatly benefit both the economy and the citizens of the Union. By developing a standardised framework for data exchanges and outlining some fundamental standards for data governance, it is vital to improve the environment for data sharing in the internal market, giving special emphasis to promoting collaboration between MS. The DGA, also known as Regulation (EU) 2022/868 on European Data Governance, was therefore enacted by EU legislators on May 30, 2022. This regulation establishes a) requirements for the reuse of specific categories of data held by public sector organisations within the Union; b) a framework for notification and oversight of the provision of data intermediation services; c) a framework for the voluntary registration of entities that collect and process data made available for altruistic purposes; and d) a framework for the creation of a European Data Innovation Board. The DGA does not impose any requirements on public sector organisations to permit the reuse of data or exempt them from their legal obligations to maintain confidentiality under Union or national law. The DGA is unaffected by a) specific provisions in Union or national law regarding the access to or re-use of certain categories of data, particularly concerning the granting of access to and disclosure of official documents; and b) public sector organisations' legal obligations to permit the re-use of data or to requirements related to the processing of non-personal data. The provisions of any sector-specific Union or national law that demand compliance with specific additional technical, administrative, or organisational requirements, including through an authorisation or certification regime, should also apply to public sector organisations, data intermediation service providers, or recognised data altruism organisations. Any such specified additional requirements should be reasonable, not discriminatory, and supported by facts. Any personal data processed in conjunction with this Regulation should be subject to Union and national law on the protection of personal data. The Regulation (EU) 2016/679 and (EU) 2018/1725, as well as Directives 2002/58/EC and (EU) 2016/680, are specifically unaffected by the DGA, including in terms of the authority and jurisdiction of supervisory authorities. The applicable Union or national law on the protection of personal data should take precedence in the event of a disagreement between the DGA and such Union law or national law implemented in line with such Union law. The rights and obligations outlined in Regulations (EU) 2016/679 or (EU) 2018/1725, as well as Directives 2002/58/EC or (EU) 2016/680, are not affected by the DGA, nor does it establish a legal basis for the processing of personal data. The DGA has no bearing

on how competition law is applied or on the MS' rights to engage in public safety, defence, and national security-related activities. The DGA is going to apply from September 24, 2023.[591]

Data is a crucial resource for securing green and digital transitions and a fundamental part of the digital economy. In recent years, both humans and machines have been producing increasingly more data. However, the majority of data remain inactive or their value is concentrated in a small number of significant businesses. Low trust, competing economic motivations, and technological barriers prevent data-driven innovation from reaching its full potential. To ensure that everyone takes advantage of these opportunities, it is crucial to unlock this potential by presenting opportunities for data reuse and by removing obstacles to the growth of the European data economy following European laws and in complete acceptance of European values. The European Strategy for Data[592], adopted in February 2020, was one of several strategic goals outlined in the Commission Work Programme 2020. With this strategy, Europe will become a worldwide leader in the data-agile economy and create a true single market for data. The Commission urged to present the Data Act - the second significant project of the data strategy, to promote and enable a greater and fairer flow of data in all sectors, including B2B, B2G, G2B, and G2G, in the European Parliament's resolution on a European strategy for data on March 25, 2021. To ensure fairness in the distribution of value from data among participants in the data economy and to promote access to and use of data, the Commission proposed the Data Act (DA) on February 23, 2022. The DA is a horizontal proposal that outlines fundamental guidelines for all industries on the rights to use data, such as in the fields of consumer goods or smart machinery. The rights and obligations of data access and use have, however, also been subject to varied degrees of regulation at the sectoral level. No such existing laws will be altered by the DA, but any new laws in these fields should, in theory, be in line with its horizontal principles. When reviewing sectoral instruments, it is important to consider whether they are in line with the horizontal rules of

[591] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance), PE/85/2021/REV/1, OJ L 152, 3.6.2022, 1–44.

[592] European Commission, 'Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions A European strategy for data', Brussels, 19.2.2020, COM (2020) 66 final, 1.

the DA. The aforementioned proposal gives vertical legislation flexibility to specify more specific guidelines for achieving sector-specific regulatory goals.[593]

By enabling businesses to reach users across the Union, by facilitating cross-border trade, and by opening completely new business opportunities to a large number of Union companies, digital services in general and online platforms, in particular, play an increasingly important role in the economy, particularly in the internal market. A small number of significant businesses that offer core platform services have arisen with significant economic influence, making them potentially eligible for gatekeeper designation. Gatekeepers have a big impact on the internal market since they operate as gateways for many corporate users to connect with consumers across the Union and on various markets. As a result, on September 14, 2022, the EU legislators adopted Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector, also known as the DMA. The purpose of the DMA is to promote the proper functioning of the internal market by establishing harmonized rules to ensure that all businesses have competitive and fair markets in the digital sector throughout the Union, where gatekeepers are present, for the benefit of business users and end users. The entity providing core platform services is referred to as a 'gatekeeper' and is thus designated following Art.3 if: a) it significantly affects the internal market; b) it offers a fundamental platform service that serves as a crucial gateway for business users to connect with end-users; c) it currently has an entrenched and durable position in its business activities, or it will likely do so soon. Under Art.2(2), the concept of the 'core platform service' means any of the following: a) online intermediation services; b) online search engines; c) online social networking services; d) video-sharing platform services; e) number-independent interpersonal communications services; f) operating systems; g) web browsers; h) virtual assistants; i) cloud computing services; j) online advertising services, including any advertising networks, advertising exchanges and any other advertising intermediation services. The DMA became effective from May 2, 2023. The Commission should assess DMA by 3 May 2026, and then every three years thereafter, and report to the European Parliament, the Council, and the European Economic and Social Committee. The evaluations should analyse whether the DMA's goals of guaranteeing competitive and fair markets have

[593] European Commission, 'Proposal for a Regulation of The European Parliament and Of The Council on harmonised rules on fair access to and use of data (Data Act)', Brussels, 23.2.2022, COM (2022), 68 final 2022/0047 (COD), 2.

been met, as well as the impact of the DMA on business users, particularly SMEs, and end users.[594]

The DMA is based on the current P2B legislation, without being in contradiction with it, as is emphasised in the DMA proposal. The definitions proposed in the DMA, particularly those for 'online intermediation services' and 'online search engines,' are consistent with P2B Regulation. Additionally, DMA is completely consistent with the proposed Digital Services Act. The DSA is a horizontal initiative that focuses on issues like the responsibility of online intermediaries for content created by third parties, user safety online, or asymmetric due diligence requirements for various information society service providers depending on the type of societal risks those services pose. The DMA instructions, in contrast, is concerned with economic inequalities, unfair commercial practices by gatekeepers, and their undesirable effects, including weakened contestability of platform markets. In its contribution to creating a just and competitive digital economy - one of the three fundamental pillars of the policy orientation and objectives established in the Communication 'Shaping Europe's Digital Future' - the DMA's proposal is consistent with the Commission's digital strategy. Additionally, the DMA's proposal strengthens current EU (and national) competition laws. The DMA's proposal is also in line with other EU legal frameworks, such as the GDPR, the EU's acquis of consumer protection laws, the EU Charter, and the European Convention of Human Rights.[595]

New and innovative information society (digital) services have appeared since the passage of the ECD 2000/31/EC, changing the daily lives of Union citizens and influencing and reshaping how people connect, interact, consume, and conduct business. These services have made significant contributions to societal and economic changes in the Union and around the world. However, using those services has also given rise to new dangers and difficulties for both societies at large and the users of those services. The Commission pledged to update the horizontal regulations that outline the duties and obligations of suppliers of digital services, and online platforms in particular, in the Communication 'Shaping Europe's Digital Future'. Based on Art.225 of the TFEU, the European Parliament adopted two

[594] Regulation (EU) 2022/1925, OJ L 265, 1–66

[595] European Commission, 'Proposal for a Regulation of The European Parliament and of The Council on contestable and fair markets in the digital sector (Digital Markets Act)', Brussels, 15.12.2020, COM (2020), 842 final, 2020/0374 (COD), 3.

resolutions: 'Digital Services Act: Adapting Commercial and Civil Law Rules for Commercial Entities Operating Online' and 'Digital Services Act: Improving the Functioning of the Single Market.' [596]

Therefore, on October 19, 2022, the EU legislators adopted the Regulation (EU) 2022/2065 on a Single Market for Digital Services, also known as the DSA, to protect and improve the functioning of the internal market. By establishing standardised guidelines for a secure, reliable, and trusted online environment that promotes innovation and in which fundamental rights enshrined in the EU Charter, including the principle of consumer protection, the DSA seeks to contribute to the proper functioning of the internal market for intermediary services. In the internal market, the DSA establishes standardised regulations for intermediary service delivery. It establishes, in particular: a) a framework for the conditional exclusion of intermediary service providers from responsibility; b) rules on particular due diligence requirements targeted to select specific groups of intermediary service providers; and c) guidelines for putting this Regulation into effect and enforcing it, including those about the coordination and cooperation of the competent authorities. The DSA applies to intermediary services provided to service recipients who have their place of business or are located in the Union, regardless of where the providers of those intermediary services have their place of business. Regardless of whether the service is delivered using an intermediate service, the DSA should not apply to any services that are not intermediary services or to any restrictions imposed concerning such services. The DSA should not have an impact on how Directive 2000/31/EC is applied. The DSA establishes obligations as well as a system of transparency and accountability for providers of intermediary services, including a) internet access providers; b) hosting services, such as cloud computing and web hosting; c) domain name registrars; d) online marketplaces; e) app stores; f) social networks; g) content sharing platforms; and h) online travel and lodging platforms. The DSA applies to online platforms and online search engines that are classified as very large online platforms or very large online search engines and have an average monthly active user base in the Union that is equal to or higher than 45 million. The DSA requirements aim to minimise harmful online content and protect all parties, especially minority groups, from targeted advertising

[596] European Commission, 'Proposal for a Regulation of The European Parliament and Of The Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC', Brussels, 15.12.2020, COM (2020), 825 final, 2020/0361 (COD), 1-2.

practices, illegal content, and online hate speech. The DSA should become effective on February 17, 2024. Articles 24(2), (3), and (6), Art.33(3) to (6), Art.37(7), Art.40(13), Art.43, and Sections 4, 5, and 6 of Chapter IV, on the other hand, should take effect on November 16, 2022.[597]

Artificial intelligence refers to a system that by analysing the environment and taking action exhibits intelligent behaviour with some degree of autonomy to achieve specific goals. AI systems can either be based on software such as voice assistants, search engines, speech and facial recognition systems, or hardware-implanted devices such as advanced robots, autonomous cars, drones, or Internet of Things applications.[598] AI is a rapidly expanding family of technologies that has the potential to provide a wide range of economic and societal benefits across a wide range of sectors and social activities. AI may assist socially and environmentally positive results while also providing important competitive benefits to businesses and the European economy by enhancing prediction, optimising operations and resource allocation, and personalising service delivery. Given the rate of technological progress and potential obstacles, the EU is committed to pursuing a balanced approach. It is in the Union's best interests to maintain the EU's technological dominance and to ensure that new technologies are developed and implemented following Union values, fundamental rights, and principles. The Commission released the White Paper on AI, the EU approach to excellence and trust on February 19, 2020. The White Paper outlines policy alternatives for achieving the dual goals of encouraging the adoption of AI and addressing the hazards related to some applications of this technology. The proposal on AI Act dated 21.4.2021, which proposes a legal framework for trustworthy AI, aims to implement the second objective for the establishment of an ecosystem of trust. The proposal, which is founded on EU principles and fundamental rights, intends to inspire firms to create AI-based solutions while giving consumers and other users the confidence to use them. The proposal creates a solid but adjustable legal foundation. On the one hand, it makes basic regulatory decisions that are thorough and future-proof, such as the standards that AI systems must adhere to. On the other hand, it establishes a proportionate regulatory framework centred on a clearly defined risk-

[597] Regulation (EU) 2022/2065, OJ L 277, 1–102.
[598] European Commission, 'Communication from The Commission to The European Parliament, The European Council, The Council, The European Economic and Social Committee and The Committee of The Regions: Artificial Intelligence for Europe Brussels', Brussels, 25.4.2018, COM (2018) 237 final, 1.

based regulatory approach that does not impose needless barriers to trade, whereby legal intervention is tailored to those specific circumstances where there is a legitimate basis for concern or where such concern can be reasonably anticipated shortly. The legal framework also has adaptive features that allow it to adjust on demand as new challenging circumstances arise and technology advances.[599] The Regulation could start to apply to operators as early as the second half of 2024 if the standards are established and the initial conformity assessments have been completed.[600]

The specific difficulties AI poses to current liability laws were also noted by the Commission in the Report on AI Liability[601] that accompanied the White Paper. The processing of liability claims for damage caused by AI-enabled products and services is not appropriate under current national liability laws, particularly those based on fault. Such laws require victims to demonstrate that the person who caused the harm committed an illegal act or omitted to do so. Complexity, autonomy, and opacity (the so-called 'black box' effect), which are particular to AI, may make it difficult or prohibitively expensive for victims to identify the responsible party and establish the necessary elements for a successful liability claim. In comparison to cases without AI, victims may face much longer legal proceedings and very large upfront expenditures while pursuing compensation. Therefore, victims may be discouraged from filing a claim at all. To encourage the adoption of reliable AI and reap its full benefits for the internal market, a proposal for a Directive on AI Liability (AILD) on September 28, 2022, was introduced. The Commission has suggested rules in the AI Act proposal that aim to lessen safety concerns and safeguard fundamental rights. Both safety and liability apply at various times and reinforce one another. They are two sides of the same coin. By recommending adjustments to the producer's liability for faulty products under the Product Liability Directive as well as the targeted harmonisation under this proposal, the Commission adopts a comprehensive approach to liability in its AI strategy. Since claims falling under these areas deal with various sorts of liability, these two policy initiatives are

[599] European Commission, 'Proposal for a Regulation of The European Parliament and of The Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts', Brussels, 21.4.2021, COM/2021/206 final, 1-3.

[600]Regulatory framework proposal on artificial intelligence <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> accessed 10 Aug. 2023.

[601] European Commission, 'Report from the Commission to the European Parliament, the Council and the Economic and Social Committee on the safety and liability implications of artificial intelligence, the internet of things and robotics', Brussels, 19.2.2020, COM (2020) 64 final, 1.

intertwined and function as a package. The Product Liability Directive addresses producer no-fault liability for defective items, which results in payment for specific categories of losses, primarily suffered by persons. This proposal, on the other hand, addresses national liability claims that are primarily attributable to an individual to compensate for every kind of damage and any kind of victim. Together, they establish a comprehensive, efficient system of civil liability. Jointly these rules will increase public confidence in AI by guaranteeing that victims are fairly compensated if harm happens despite the AI Act's and other regulations' preventive measures.[602]

5.2.4. Summary

The digital transformation of the EU is an inevitable result of technological advances and digital trends in global markets. In addition to them, external factors such as the economic crisis and the pandemic have also accelerated the process of digitalisation of the EU society and economy. As the EU needs to maintain its digital leadership in a competitive marketplace, robust and innovative strategies are also required between MS. The DSM Strategy is a prime example of the EU's attitude towards strengthening the single and sovereign market based on common EU values and principles. The current legislative approaches of the EU show that, based on common values and principles, the need of EU citizens have always been, are and will be on the agenda of the DSM Strategy. In addition, the commitment of the EU to continue promoting this strategy can be seen in recent initiatives and implemented legislation.

As part of the European Data Strategy, the adopted DGA and the proposed DA point to a promising future in the creation and strengthening of a single market for data space in the EU. Data, as the cornerstone of this digital transformation, also serves as a tool to create an agile and data-driven economy for the benefit of stakeholders. While the DGA enables a voluntary way to manage data sharing and reuse, the proposed DA, on the other hand, specifies who can use and access what data for what purposes within the EU. In addition, the former is trying to create a trusting environment for consumers, and the latter is engaged in providing consumers with fair access to data collected across industries. Both DGA and DA

[602] European Commission, 'Proposal for a Directive of The European Parliament and Of The Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)', Brussels, 28.9.2022, COM (2022), 496 final 2022/0303 (COD), 1.

strive to create a human-centric and transparent online environment for consumers and businesses across the EU.

The further digital cutting-edge efforts to reduce the digital divide and bring Europe into line with the digital age are the DMA and DSA. While the DMA strives to ensure a contestable and fair digital market by setting a set of obligations on gatekeepers, the DSA indicates rules on the liability of providers of online intermediary services and safeguards their diligence and sets more extensive obligations on online platforms and large online platforms. The former is typically connected with competition law and market access, whereas the latter is generally related to consumer protection and liability issues.

As a new era is dawning in the digital sector with the advent of AI, new measures and frameworks are needed to maintain the EU's digital leadership in digital markets. Since the way AI is now characterized will later represent the entire future of the EU society and economy, new proposed AI-related laws may become an acceptable global model for other countries. As the proposed AI Act is the first horizontal legal framework of its kind, it is commendable that it encourages all businesses to develop AI-based solutions by addressing the threats to fundamental rights and safety. This proposed Act, while providing a technology-neutral definition of AI, seeks to create robust AI systems for consumers and open access to innovation and investment for businesses in the digital marketplace. The next proposed major initiative - the AILD introduces new rules specifically for damage caused by AI systems. This proposed AILD ensures that people harmed by AI systems receive the same level of protection as people harmed by other technologies in the EU. By emphasising the rebuttable presumption of causality, the proposed AILD intends to reduce the burden of proof for victims in determining the harm caused by an AI system. Both of these proposed acts serve to create an AI-enabled environment and prepare consumers to feel confident and secure in exercising their fundamental rights based on EU values and principles.

Overall, there is no doubt about the EU's ability to legislate and establish uniform standards for all persons living in its MS. The primary concern is how much of this capacity the EU can currently execute and accomplish depending on market demand and sectoral developments. The emphasis will be on defining the extent to which the EU is capable of regulating the digital sector, keeping in mind that e-commerce and all online-related areas are possible to encompass under the umbrella of the digital sectors. In general, contemporary

digital breakthroughs and technological progress are closely tracking the EU's digital industry. As a result, based on the most recent proposed legislative acts and directives, it is expected to notice that the EU is now on the verge of a disorganised and complicated digital revision and transformation of the legislative basis phase.

It also shows that as one of the digital regions of technological advances, the EU urgently needed these modifications and reforms, just to keep up with its giant global regional rivals. Although the reasons and causes for these legal reforms may be diverse and even unrelated, the demand and need for these transitions in the digital economy must take precedence. Europe's Digital Decade, with digital ambitions for 2030, demonstrates that the EU must reform its digital regulatory legislative frameworks for the sake of a human-centric, trustworthy, and sustainable environment for all stakeholders.

Given the competitive nature of the digital world, it is no surprise that the EU is eager to advance its DSM Strategy to the maximum level to avoid falling behind these digital races. For this reason, the EU's efforts to keep track of the latest digital revolutions and transformations are commendable and exemplary in maintaining the EU's position as a market leader in this area. Additionally, these legal reformations for the digital age will help the EU prepare for potential future problems and ensure that all internet users feel safe and secure while interacting with others. Needless to say, there are still many adjustments waiting for the EU in the form of submitted enactments, evaluation reports and stakeholder workshops regarding the implementation and application of the recently adopted regulations, directives and acts. Between the proposed legal acts and their enforcement deadlines, the EU would have the opportunity to find out the mistakes, inconsistencies and reasonable demands of the stakeholders in terms of the implementation of these legal acts in the future. Furthermore, there is always a potential that the proposed legislations would one day have the same 'Brussels effect' as the GDPR[603], which was the result of its implementation and application not just in the EU but also globally. This Brussels effect would point to the world of EU strategy standards of the DSM, global regulatory power and the next benchmark case for the implementation of further legislative reforms.

[603] Andrea Renda, 'Beyond the Brussels Effect,' *FEPS*, Belgium, Policy Brief, March 2022, 4.

Chapter 6. Conclusion

This dissertation concludes with some recommendations for future advances to ensure that online users, whether online consumers or data subjects, interact at the highest level of security set by the EU.

6. Conclusion and recommendations

Since one of the main rational motives for solving the research questions was the study of e-commerce, it can be said without exaggeration that e-commerce cannot be limited to one discipline, since it is characterized by a variety of options and infrastructure components supported by technologies. In order to explore the potential and future prospects of e-commerce, it is advisable to consider it as a separate discipline and not as a sub-area of e-business law. The final line is that whether it is online commerce or digital commerce, processes are the same in their fundamental operation and structure and should be regarded as terms that are commonly used interchangeably. Due to its distinct qualities as a multidisciplinary topic, e-commerce law has incorporated this potential into its systems and applications. All elements, especially e-commerce systems and e-commerce applications, must be integrated, interact and function simultaneously for the constant and consistent development of e-commerce in order to achieve the desired results and avoid unforeseen problems. The most recent regulatory changes in digital services and online marketplaces demonstrate the ongoing efforts of the e-commerce industry to keep up with the most recent internal market digital transformation. Therefore, since it covers businesses, organisations, and individuals, it is logical to consider e-commerce as a separate field with several levels of interaction.

No two people are the same, so they can be distinguished by characteristics such as mental or physical instability, age, gender, and credulity, among other things. These distinguishing features show that while not all people can be classified as normal or standard, some people can be excluded from the group. When connecting with others online, individuals with these typical traits could feel more susceptible and vulnerable. Since there wasn’t a complete definition of the term vulnerability, it was required to search for one and

evaluate the ones that academics have already put out. Here are some results of the research work based on the findings of the research questions:

1) To what extent can the EU define the concept of vulnerability and the position of vulnerable individuals in consumer protection law.

The EU has somehow managed to create a static, stable definition of the vulnerable consumer category, although it is only developed from the perspective of the UCPD. So, the vulnerable group of consumers is defined as a clearly identifiable group based on mental or physical disability, age or credulity, and the trader can reasonably be expected to 'foresee their vulnerability'. Despite the EU's efforts to define vulnerable consumers, this definition is devoid of situational and inherent elements, which are, naturally, crucial components of different consumer groupings. Another reason for this definition is that it does not accurately reflect the digital capabilities of vulnerable or online consumers, making it impossible to assess their current worth in the online marketplace. As a result, consumer protection laws and policies that include vulnerable consumers are not applicable to other consumer-related online industry practises, such as contractual relationships or dispute resolution circumstances.

The UCPD is no longer up to date to provide an adequate definition of the vulnerable consumer group that should be proportionate to the recent digital revolution, particularly by using the average consumer group as a benchmark for consumer protection law. A guide to using a vulnerable consumer group, not only in commercial practices but also in other industries, should consider a consistent and coherent approach directly in formulating digital vulnerability criteria. Particularly in view of the explosive growth of information technology, the position and availability of the most vulnerable group of consumers must be adequately adjusted to the concerns of the modern DSM. As recommendations for the future, particularly for greater performance and realistic contribution, the legislators should identify the characteristics of particularly digitally vulnerable consumer groups and their proclivity to be particularly vulnerable to particular commercial practises.

So, according to the legal framework for EU consumer protection, it is recognized that the EU's consumer regulatory mechanisms are more effective at defining and safeguarding the typical average group of consumers, both in theory and in practice. It is practically very difficult for vulnerable consumers to acknowledge whether they require protection from

unfair commercial practices, despite provisions for them in EU consumer protection law. These vulnerable consumer groups will always require additional guidance and support in online transactions since they do not receive reliable information or this is not achievable owing to extrinsic and intrinsic causes.

Based on the CRD and the UCPD, some recommendations should be taken into account to protect vulnerable individuals under the EU consumer protection law:

a) Provide clear and transparent information. Sellers and service providers should provide vulnerable consumers with clear and understandable information about their products or services. This includes information about prices, terms and conditions, and any potential risks or side effects.

b) Avoid aggressive or misleading sales practices. Companies should not use misleading or aggressive sales tactics that take advantage of vulnerable consumers. This includes avoiding pressure selling, hidden fees or charges, and false claims about a product or service.

c) Ensure accessibility. Companies must ensure that their products and services are accessible to all consumers, regardless of their vulnerabilities and shortcomings. This includes providing information in alternative formats such as braille or audio, and offering assistance to consumers with disabilities.

d) Offer refunds or the right to cancel. Companies should offer refunds or the right to cancel for vulnerable consumers who may have made a purchase by mistake or who are experiencing financial hardship.

e) Provide proper customer service. Companies must provide adequate customer service to assist vulnerable consumers with any questions or concerns they may have regarding their purchase or service. This includes offering multiple customer support channels such as phone, email, and live chat.

2) To what extent can EU explain the concept of vulnerability and the position of the vulnerable individuals in the data protection law.

Since consumers and data subjects are in a weaker position in each of these areas due to their status, it is reasonable to put forward an average concept of the data subject as a starting point in data protection law similar to consumer protection law. The mention of vulnerable natural persons implies that the data controller may occasionally rely on non-

vulnerable individuals as average or standard data subjects, even though the GDPR treats all data subjects equally and applies the data processing laws to all of them. The requirement to identify the status of average data subjects is also driven by the significant role of the data controller in the power discrepancy resulting from information processing asymmetry. It is necessary to introduce a standard notion of the average data subject in data processing so that data subjects can more effectively exercise their rights in practice. The requirements of the GDPR are intended to preserve everyone's privacy and rights, regardless of their unique features or circumstances, which may be one of the reasons why the concept of average data subjects has not been properly explored.

Thus, in general, data protection law, in particular the GDPR, did not develop either the notion of an average data subject or the notion of a vulnerable data subject as a concept, but slightly referred to children as vulnerable natural persons. On the other hand, the absence of average data subjects in data protection regulation may also mean that vulnerable data persons remain unprotected against the background of average data subjects. Although the concept of vulnerability is unavoidably present in data protection law, it is still insufficiently recognized as a basis for defining the social differences of data subjects. It is possible to unleash the potential of the GDPR to secure the processing of personal data of various underprivileged data subjects by bringing the notion of vulnerability into data protection law, particularly in relation to data subjects. In the data processing, the category of children as vulnerable data subjects is referenced with features of parental consent and data controllers' information obligations. Data controllers, by analogy, cannot impose the same obligations on different groups of persons as vulnerable data subjects. Thus, it would be preferable if data controllers took extra precautions when processing the data of various groups of vulnerable data subjects. Therefore, if the data controller is aware that their products or services are used by (or targeted at) other vulnerable members of society, such as people with disabilities or people who might have difficulty accessing information, it should also take into account the vulnerabilities of such data subjects when deciding how to ensure that it complies with its transparency obligations concerning such data subjects. Additionally, data controllers must be aware of the nature, scope, and context of processing that could constitute serious risks to the rights and freedoms of data subjects at every stage of processing because they are responsible for the purpose and method of processing. As a result, in general, when processing

data, and being responsible and accountable, the data controllers should refrain from preying on the weaknesses of the vulnerable data subjects.

Based on the GDPR, here are a few more recommendations for protecting vulnerable individuals under data protection law:

a) Get informed consent. Companies must obtain the informed consent of vulnerable individuals before collecting, processing or sharing their personal data. This means providing clear and understandable information about the purpose of data processing, the identity of the data controller, and any potential risks or consequences of data processing.

b) Provide access and control to data. Companies must provide vulnerable individuals with access to their personal data and the ability to control how their data is used. This includes the right to request the erasure of data, data portability and restrictions on data processing.

c) Ensure security of data. Companies must ensure the security of the personal data of vulnerable individuals, including the adoption of appropriate technical and organisational measures to protect against unauthorized access, disclosure or loss.

d) Provide transparency of processing. Companies should provide vulnerable individuals with transparent information about their data processing activities, including the categories of personal data collected, the purposes of the processing and the recipients of personal data.

e) Monitor and report data breaches. Companies should monitor data breaches and report them to the relevant authorities and the affected vulnerable individuals. This includes providing clear and understandable information about the nature and extent of the violation, as well as the potential risks or consequences for affected vulnerable individuals.

3) To what extent can EU e-commerce deal with recent regulatory issues?

As a result of technological breakthroughs and emerging digital market trends, the EU is unavoidably going through a digital revolution. The epidemic and the economic crisis have hastened the digitalisation of the EU's society and economy along with them. If the EU is to maintain its position as a market leader in the digital sphere, strong and innovative measures by MS are also required. A brilliant model for the EU's approach to strengthening the sovereign single market, based on common EU values and principles, is the DSM Strategy. The DSM strategy will continue to prioritize fulfilling the needs of EU citizens, as it is based

on common values and principles. The DGA and the proposed Data Act, which are both components of the European Data Strategy, indicate a bright future for building and enhancing the EU's single market for data space. The DMA and the DSA represent additional cutting-edge initiatives to close the digital divide and bring Europe into the digital era. AI is ushering in a new era in the digital sector, and new policies and frameworks like the AI Act and the AIL Directive are required to keep the EU at the forefront of the digital economy.

The EU digital industry usually tries to keep a close eye on modern technologies and digital advances. Accordingly, based on the most recent proposed legislative acts and directives, it is predicted that the EU is currently on the verge of a disconnected and complex digital review and transformation of the legal frameworks. It also shows how urgently the EU requires these changes and reforms to keep up with its sizable regional rivals on the global stage and remain one of the key hubs of technology innovation. Regardless of how different and sometimes even unrelated the reasons and explanations for these legislative reforms may be, the desire and necessity for these changes in the digital economy must come before any other concerns. As shown by Europe's Digital Decade and its digital ambitions for 2030, the EU must update its digital regulatory legislative frameworks to establish a human-centric, trustworthy, and sustainable environment for all stakeholders. It is not surprising that the EU is committed to developing its DSM Strategy at the highest level, given the capitalist nature of the digital world, to keep up with these digital races. Therefore, the EU's efforts to keep track of the most recent digital revolutions and changes are admirable and appropriate in terms of maintaining the EU's position as an industry leader in this regard. These legal updates for the digital age will also help the EU prepare for potential future challenges and ensure that everyone who uses the Internet feels safe and secure. Still, the EU has many adjustments to come in the form of proposed and submitted regulations, evaluation reports and stakeholder workshops on the implementation and application of adopted regulations, directives, and acts. The EU would have the chance to spot any errors, incompatibilities, or valid stakeholder demands concerning the future execution of these legal acts between the proposed legal acts and their implementation deadlines. Furthermore, there's always a potential that the proposed legislations will one day experience the same 'Brussels effect' as the GDPR, which was approved not just in the EU but also internationally. The Brussels effect would highlight the

EU's strategic requirements for the DSM and the global regulatory authority for enacting additional legislative reforms.

Bibliography

Books and edited works

Abraham L. Newman, *Protectors of Privacy: Regulating Personal Data in the Global Economy,* Ithaca, Cornell University Press, 2008.

Algharabat R. S. et al., 'Investigating the Impact of Social Media Commerce Constructs on Social Trust and Customer Value Co-creation: A Theoretical Analysis' in N. P. Rana et al. (eds.), *Digital and Social Media Marketing, Advances in Theory and Practice of Emerging Markets,* Switzerland, Springer Nature AG, 2020.

Ananda Mitra, *Digital Security: Cyber Terror and Cyber Security,* New York, Chelsea House, 2010.

Ashton David et al., 'EU Mapping: Overview of Internal Market and Consumer Protection related legislation, publication for the Committee on Internal Market and Consumer Protection', Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, European Union, 2023.

Ausloos Jef, *The Right to Erasure in EU Data Protection Law from Individual Rights to Effective Protection,* Oxford University Press, Oxford, 2020.

Awad Elias M., *Electronic Commerce: From vision to fulfillment,* New Jersey, Pearson Education, Inc., 2004.

Bacchetta Marc et al (ed)., 'Electronic commerce and the role of the WTO', WTO Special Studies, No. 2, WTO, Geneva, 1998.

Bakhoum Mor et al., 'Introducing a Holistic Approach to Personal Data' in Mor Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law, MPI Studies on Intellectual Property and Competition Law 28*, Germany, Springer-Verlag GmbH, 2018.

Barocelli Sergio Sebastián 'Consumer Protection and Sharing Economy' in D. Wei et al. (eds*.), Innovation and the Transformation of Consumer Law,* Singapore, Springer Nature Pte Ltd., 2020.

Basu Subhajit, *Global Perspectives on E-Commerce Taxation Law: Markets and the law,* Ashgate Publishing Limited, Hamphsire, 2007.

Benau P. & V. Bitos, 'Developing Mobile Commerce Applications' in Wen-Chen Hu (ed*) Selected Readings on Electronic Commerce Technologies: Contemporary Applications,* Information Science Reference, Hershey, 2009.

Bhajaria Nishant, *Data Privacy*, Manning Publications Co., Shelter Island, 2022.

Bhasker Bharat, *Electronic Commerce: Framework, Technologies and Applications,* India, McGraw Hill Education, 2013.

Bhattacherjee Anol, *Social Science Research: Principles, Methods, and Practices,* Textbooks Collection 3, 2012.

Bidgoli Hossein, *Electronic Commerce: Principles and Practice*, USA, Academic Press, 2002.

Braynov Sviatoslav 'E-Commerce Vulnerabilities' in Hossein Bidgoli (ed) *Handbook of the Information Security: Threats, Vulnerabilities, Prevention, Detection, and Management,* vol.3, Hoboken, John Wiley & Sons, Inc., 2006.

Burnham Bill, *How to Invest in E-Commerce Stocks,* USA, The McGraw-Hill Companies Inc., 1999.

Bwalya Kelvin Joseph & Stephen Mutula, *E-Government: Implementation, Adoption and Synthesis in Developing Countries*, Berlin, Walter de Gruyter GmbH, 2014.

Bygrave Lee A. & Luca Tosani 'Article 4(11). Consent' in Christopher Kuner, Lee A. Bygrave and Xe Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary,* New York, Oxford University Press, 2020.

Cartwright Peter 'The consumer image within EU law' in Christian Twigg-Flesner (ed) *Research Handbook on EU Consumer and Contract Law*, Cheltenham, Edward Elgar Publishing Limited, 2016.

Celia T. Romm & Fay Sudweeks (eds), *Doing Business Electronically: a global perspective of electronic commerce*, London, Springer-Verlag Limited, 2000.

Chaffey David, *Digital Business and E-commerce management: Strategy, implementation and practice*, Pearson, 2015.

Chan Henry et al, *E-commerce: Fundamentals and Applications*, Chichester, John Wiley & Sons Ltd, 2001.

Chen Hu Wen (ed), *Selected Readings on Electronic Commerce Technologies: Contemporary Applications, Hershey*, Information Science Reference, 2009.

Cheng Hsu and Somendra Pant, *Innovative Planning for Electronic Commerce and Enterprises: A Reference Model*, Dordrecht, Kluwer Academic Publishers, 2000.

Chesher Michael, Rukesh Kaura & Peter Linton, *Electronic Business & Commerce*, London, Springer-Verlag, 2003.

Combe Colin, *Introduction to E-business Management and strategy*, Oxford, Elsevier Ltd, 2006.

Dahlberg E. et al., 'Legal obstacles in Member States to Single Market rules', Publication for the committee on Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2020.

Davidson Alan, *The law of electronic commerce*, Cambridge, Cambridge University Press, 2009.

De Franceschi Alberto (ed) European Contract Law and the Digital Single Market. The Implications of the Digital Revolution: Current Issues and New Perspectives', Cambridge, Intersentia Ltd, 2016.

De Streel Alexendre et al., 'Contribution to growth: The European Digital Single Market, Delivering economic benefits to citizens and businesses', Study for the Committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2019.

De Terwangne Cecile 'Article 5. Principles relating to processing of personal data' in Christopher Kuner, Lee A. Bygrave & Xe Christopher Docksey *The EU General Data Protection Regulation (GDPR): A Commentary*, New York, Oxford University Press, 2020.

Deirdre M. Curtin & Ige F Dekker, 'The European Union from Maastricht to Lisbon: Institutional and Legal Unity out of the shadows', in Paul Craig & Grainne De Burca (eds) *The Evolution of EU law*, New York, Oxford University Press Inc., 2011.

Edwards Lilian (ed) *The New Legal Framework for E-Commerce in Europe*, Oregon, Hart Publishing, 2005.

Fairhurst John, *Law of the European Union*, UK, Pearson Education Limited, 2016.

Fink Arlene, *Conducting research literature reviews: From the Internet to Paper*, California, SAGE Publications Inc., 2014.

Fuster Gloria González ‘Article 18. Right to restriction of processing’ in Christopher Kuner, Lee A. Bygrave and Xe Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary,* New York, Oxford University Press, 2020.

Gordijn J., H. Bruin & H. Akkermans, ‘Integral Design of E-commerce Systems: Aligning the Business with Software Architecture through Scenarios’ in H. de Bruin(ed) *ICT-Architecture in the BeNeLux,* 1999.

Graef Inge, ‘Blurring Boundaries of Consumer Welfare: How to Create Synergies Between Competition Consumer and Data Protection Law in Digital Markets’ in Mor Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law, MPI Studies on Intellectual Property and Competition Law 28,* Germany, Springer-Verlag GmbH, 2018.

Helberger Natali et al., *EU Consumer Protection 2.0: Structural asymmetries in digital consumer markets,* Brussels, 2021.

Hernández B., J. Jiménez & M.J. Martín, ‘Analysis of the Relationship Existing between Business Commercial Information Technologies’ in I. Lee (ed), *Transforming E-Business Practices and Applications: Emerging Technologies and Concepts,* Hershey, Information Science Reference, 2010.

Hert P. De & Gutwirth S., ‘Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action’ in S. Gutwirth et al. (eds.), *Reinventing Data Protection?* Berlin, Springer, 2009.

Howells Geraint, Christian Twigg-Flesner & Thomas Wilhelmsson, *Rethinking EU Consumer Law,* New York, Routledge, 2018.

Ismail Yasmin, ‘E-commerce in the World Trade Organization: History and latest developments in the negotiations under the Joint *Statement’ International Institute for Sustainable Development and CUTS International,* Geneva, 2020.

Jailani N. ‘Concept of an Agent-Based Electronic Marketplace’ in I. Lee (ed) *Encyclopaedia of E-Business Development and Management in the Global Economy,* Hershey, Business Science Reference, 2010.

Jansen J., L. van de Wijngaert, & W. Pieterson, ‘Channel Choice and Source Choice of Entrepreneurs in a Public Organizational Context: The Dutch Case’ in M.A. Wimmer et al.

(Eds.): *EGOV 2010, IFIP International Federation for Information Processing 2010,* LNCS 6228, 2010.

Jonsdottir Johanna, *Europeanization and the European Economic Area: Iceland's participation in the EU's policy process*, Oxon, Routledge, 2013.

Joseph Rhoda C. & David P. Kitlan, 'Key Issues in E-Government and Public Administration' in G. David Garson and Mehdi Khosrow-Pour, *Handbook of Research on Public Information Technology,* Hershey, Information Science Reference, 2008.

Kabanov Y. & L. Vidiasova 'C2G Online Trust, Perceived Government Responsiveness and User Experience: A Pilot Survey in St. Petersburg, Russia' in I. Lindgren et al. (Eds.): *EGOV 2019, LNCS 11685, IFIP International Federation for Information Processing 2019*, Switzerland, Springer Nature AG, 2019.

Kalakota Ravi & Andrew B. Whinston, *Electronic Commerce: A Manager's Guide,* USA, Addison-Wesley Longman Inc, 1997.

Kalakota Ravi & Marcia Robinson, *e-Business 2.0: a roadmap for success,* USA, Addison-Wesley Professional, 2001.

Kamra Ashish & Bertino Elisa 'Survey of Machine Learning Methods for Database Security' in J.J.P. Tsai & P.S. Yu (eds.), *Machine Learning in Cyber Trust: Security, Privacy, and Reliability*, New York, Springer Science + Business Media LLC., 2009.

Kaprou Eleni 'The legal definition of 'vulnerable' consumers in the UCPD: Benefits and limitations of a focus on personal attributes' in Christine Riefa and Séverine Saintier (eds) *Vulnerable Consumers and the Law: Consumer Protection and Access to Justice*, Oxon, Routledge, 2021.

Kosiur David, *Understanding Electronic Commerce,* Redmond, Microsoft Press, 1997.

Kranenborg Herke 'Article 2. Material scope' in Christopher Kuner, Lee A. Bygrave & Xe Christopher Docksey *The EU General Data Protection Regulation (GDPR): A Commentary,* New York, Oxford University Press, 2020.

Kuzic Joze, Julie Fisher & Angela Scollary, 'Electronic Commerce Benefits, Challenges and Success Factors in The Australian Banking and Finance Industry' *Poland, ECIS 2002 Proceedings,* 2002.

Lacka Ewelina, 'Culture Dependent Benefits of E-commerce: A Consumer Perspective' in E. Lacka et al. (eds.), *E-commerce Platform Acceptance*, Switzerland, Springer International Publishing, 2014.

Lambert Paul, A User's Guide to Data Protection: Law and Policy, UK, Bloomsbury Professional, 2020.

Laudon Kenneth C. & Carol Guercio Traver, *E-commerce 2021–2022: Business, Technology, Society*, UK, Harlow, Pearson Education Limited, 2021.

Laudon Kenneth C. & Carol Guercio Traver, *E-commerce: business, technology, society*, Boston, Pearson, 2017.

Laudon Kenneth C. & Jane P. Laudon, *Management Information Systems: Managing the digital firms*, New York, Pearson Education Inc, 2018.

Laustsen Dalgaard, The Average Consumer in Confusion-based Disputes in European Trademark Law and Similar Fictions, Switzerland, Springer Nature AG, 2020, 6.

Lavassani K. M., B. Movahedi & V. Kumar, 'From Integration to Social Media: Understanding Electronic Marketplace' in Lee (ed) *Trends in E-business, E-services, and E-Commerce: Impact of Technology on Goods, Services, and Business Transactions*, Hershey, Business Science Reference, 2014.

Legg Jesse, *Build powerful e-commerce applications using Django*, a leading Python web framework, Birmingham, Packt Publishing, 2010.

Leonard Lori N. K., 'C2C Mobile Commerce: Acceptance Factors', In Lee (ed) *Encyclopaedia of E-Business Development and Management in the Global Economy*, IGI Global, 2010.

Li Jianhong 'A Study on the Framework of the Security-Based E-commerce Applications' in Y.-H. Han et al. (eds.), *Ubiquitous Information Technologies and Applications: Lecture Notes in Electrical Engineering*, Dordrecht, Springer, vol.214,2013.

Lodder Arno R. 'Directive 2000/31 /EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market' in Arno R. Lodder and Andrew D. Murray (eds), EU Regulation of E-Commerce: A Commentary, Cheltenham, Edward Elgar Publishing Limited, 2017.

Lodder Arno R. 'The European Union and e-commerce' in Arno R. Lodder and Andrew D. Murray (eds), EU Regulation of E-Commerce: A Commentary, Cheltenham, Edward Elgar Publishing Limited, 2017.

Mačėnaitė Milda 'Protecting Children Online: Combining the Rationale and Rules of Personal Data Protection Law and Consumer Protection Law' in Mor Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law, MPI Studies on Intellectual Property and Competition Law 28,* Germany, Springer-Verlag GmbH, 2018.

Mariga Julie (ed), *Managing E-Commerce and Mobile Computing Technologies,* USA, Idea Group Publishing, 2003.

Markellou P., M. Rigou & S. Sirmakessis 'Web Personalization for E-Marketing Intelligence' in Sandeep Krishnamurthy(ed), *Contemporary research in e-marketing,* USA, Idea Group Publishing, vol.1, 2005.

McDonald Nora & Forte Andrea 'Privacy and Vulnerable Populations' in B. P. Knijnenburg et al. (eds.), *Modern Socio-Technical Perspectives on Privacy*, Switzerland, Springer Nature, 2022.

Miriyeva Narmin, 'E-Commerce in the Time of Covid-19' in: Hajdu, Gábor (szerk.) *Rendkívüli helyzetek és jog: Kalandozások a jog peremvidékén a COVID-19 apropóján* Szeged, Magyarország: Iurisperitus Kiadó, 2021.

Miriyeva Narmin, 'Security in Electronic Commerce and Online Payments' in MIRDEC-16th, International Academic Conference on Multidisciplinary Issues and Contemporary Discussions in Social Science, *Virtual/Online Conference Proceedings: Full Paper Series Rome 2020*, Mirdec & Globecos, Italy, 2020.

Mockler R. J., D. G. Dologit & M. E. Gartenfeld 'B2B E-Business' in S. A. Becker (ed), *Electronic Commerce: Concepts, Methodologies, Tools, and Applications,* Hershey, Information Science Reference, 2008.

Mohapatra Sanjay, *E-Commerce Strategy: Text and Cases,* New York, Springer, 2013.

Muller Patrice et al., European Added Value Assessment, Better Governance of the Single Market, An assessment accompanying the European Parliament's Legislative own-Initiative Report, EAVA 2/2013, Brussels, European Union, 2012.

Nabil R. Adam & Yelena Yesha (eds*), Electronic commerce; current research issues and applications,* Berlin, Springer Verlag, 1996.

Nagaty K. A., 'E-Commerce Business Models: Part 2', in I. Lee (ed) *Encyclopaedia of E-Business Development and Management in the Global Economy,* Hershey, Business Science Reference, 2010.

Nasiopoulos D. K. et al., 'Modeling of B2C Communication Strategies in Electronic Commerce' in A. Kavoura et al. (eds.*), Strategic Innovative Marketing, Springer Proceedings in Business and Economics,* Switzerland, Springer International Publishing, 2017.

O'Hara Mary 'Foreword' in Christine Riefa and Séverine Saintier(eds) *Vulnerable Consumers and the Law: Consumer Protection and Access to Justice*, Routledge, Oxon, 2021.

Pearson B., *The Loyalty Leap for B2B: Turning Customer Information into Customer Intimacy,* USA, Penguin Special, 2012.

Phinnemore David, *The Treaty of Lisbon Origins and Negotiation,* England, Palgrave Macmillan, 2013.

Piris Jean-Claude, *The Lisbon Treaty: A legal and political analysis*, UK, Cambridge University Press, 2010.

Polcak Radim 'Article 12. Transparent information, communication and modalities for the exercise of the rights of the data subject' in Christopher Kuner, Lee A. Bygrave and Xe Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary,* New York, Oxford University Press, 2020.

Politou E. et al., *Privacy and Data Protection Challenges in the Distributed Era,* Switzerland, Springer Nature AG, 2022.

Pucihar A. & M. Podlogar 'E-Marketplace Adoption Success Factors: Challenges and Opportunities for A Small Developing Country' in S. Kamel (ed) *Electronic Business in Developing countries: Opportunities and Challenges,* Hershey, Idea Group Publishing, 2006.

Qie H. & J. Liu, 'The Research on the Electronic Commerce Service Quality Indicators in C2C Field' Z. Zhang et al. (eds.), *LISS 2014 Proceedings of 4th International Conference on Logistics, Informatics and Service Science,* Berlin Heidelberg, Springer-Verlag 2015.

Radovilsky Zinovy, *Business Models for E-Commerce,* Chennai, Cognella Academic Publishing, 2015.

Ratti Matilde ‘Personal-Data and Consumer Protection: What Do They Have in Common?’ in M. Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law, MPI Studies on Intellectual Property and Competition Law28,* Germany, Springer-Verlag GmbH, 2018.

Rayport Jeffrey F. & Bernard J. Jaworski, *E-commerce,* New York, McGraw-Hill, 2001.

Riefa Christine & Saintier Séverine ‘In search of (access to) justice for vulnerable consumers’ in Christine Riefa and Séverine Saintier(eds) *Vulnerable Consumers and the Law: Consumer Protection and Access to Justice,* Oxon, Routledge, 2021.

Rijpma Jorrit J. (ed.), *The New Eu Data Protection Regime: Setting Global Standards for The Right to Personal Data Protection,* The XXIX Fide Congress in The Hague 2020 Congress Publications, Eleven International Publishing, The Hague, 2020.

Room Stewart ‘The rights of data subjects’ in Stewart Room (ed) *Data Protection and Compliance,* Swindon, UK, BCS Learning and Development Ltd, 2021.

Rothchild John A., *Research Handbook on Electronic Commerce law,* Cheltenham, Edward Elgar Publishing Limited, 2016.

Savin Andrej, *EU Internet Law,* Edward Elgar Publishing Limited, Cheltenham, 2013.

Schneider Gary P., *E-commerce,* Boston, Cengage Learning, 2017.

Schulte-Nölke Hans et al., T’he legal framework for e-commerce in the Internal Market’, Study for the committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2020.

Shareef Mahmud Akhter et al., *The proliferation of the Internet Economy: E-Commerce for Global Adoption, Resistance, and Cultural Evolution,* Hershey, Information Science Reference, 2009.

Shaw M. et al(eds), *Handbook on Electronic Commerce,* Heidelberg, Springer, 2000.

Sherif Mostafa Hashem, *Protocols for Secure Electronic Commerce,* CRC Press, Boca Raton, 2016.

Sherif Mustafa Hashem, *Protocols for Secure Electronic Commerce,* AT&T Laboratories, Boca Raton, New Jersey Series, CRC Press LLC, 2004.

Simon Alan R. & Steven L. Shaffer, *Data Warehousing & Business Intelligence for e-commerce,* San Francisco, Morgan Kaufmann Publishers, 2001.

Sims Lisa, *Building Your Online Store with WordPress and Woo Commerce: Learn to Leverage the Critical Role E-commerce Plays in Today's Competitive Marketplace*, USA, Apress Media LLC, 2018.

Smith Kenneth & John Paul Kawalek. 'Business ethics and E-Commerce in contemporary society' in *Re-Imaging Business Ethics: Meaningful Solutions for a Global Economy,* 2015.

Stair Ralph M. & George W. Reynolds, *Principles of Information Systems,* USA, Cengage Learning, 2018.

Stair Ralph M. & Reynolds George W., *Fundamentals of Information Systems,* Boston, Cengage Leaning, 2016.

Steven O. Kimbrough & D.J. Wu (eds), *Formal Modelling in Electronic Commerce,* Berlin, Springer, 2005.

Tang Puay et al (eds), *The Impact of Electronic Commerce on the Competitiveness of SMEs in the EU,* European Parliament Directorate General for Research Directorate, 2000.

Tassabehji Rana, *Applying E-Commerce in Business,* London, SAGE Publications, 2003.

Tawfik Jelassi & Francisco J. Martínez-López, *Strategies for e-Business; Concepts and Cases on value creation and digital Business transformation,* Switzerland, Springer Nature, 2020.

Tawfik Jelassi, Albrecht Enders & Francisco J. Martínez-López, *Strategies for e-Business Creating value through electronic and mobile commerce Concepts and Cases,* Edinburgh, Pearson Education Limited, 2014.

Turban E., L. Volonino & G. Wood, *Information Technology for Management Advancing Sustainable, Profitable Business Growth,* USA, Wiley, 2013.

Turban Efraim et al., *E-commerce: A managerial and social networks perspective*, Switzerland, Springer, 2017.

Turban Efraim et al., *Electronic Commerce 2018: A Managerial and Social Networks Perspective*, Switzerland, Springer, 2018.

Turban Efraim et al., *Electronic Commerce: A Managerial and Social Networks Perspective,* Switzerland, Springer, 2015.

Turban Efraim et al., *Information Technology for Management: Advancing Sustainable, Profitable Business Growth,* US, Wiley, 2013.

Turban Efraim et al., *Introduction to Electronic Commerce and Social Commerce*, Springer, Switzerland, 2017.

Turban Efraim et al., *Social commerce: Marketing, Technology and Management,* Switzerland, Springer, 2016.

Ursic Helena, 'The Failure of Control Rights in the Big Data Era: Does a Holistic Approach Offer a Solution?' in Mor Bakhoum et al. (eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law, MPI Studies on Intellectual Property and Competition Law 28,* Germany, Springer-Verlag GmbH part of Springer Nature,2018.

Van Boom Willem H. 'Unfair commercial practices' in Christian Twigg-Flesner (ed) *Research Handbook on EU Consumer and Contract Law,* Cheltenham, Edward Elgar Publishing Limited, 2016.

Voigt Paul & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) A Practical Guide,* Switzerland, Springer International Publishing AG, 2017.

Vrabec Helena U., *Data Subject Rights under the GDPR With a Commentary through the Lens of the Data-driven Economy,* UK, Oxford University Press, 2021.

Walden Ien & Julia Hornle, *E-commerce law and practice in Europe*, Cambridge, Woodhead publishing editing Limited, 2001.

Wang Faye Fangfei, *Internet Jurisdiction and choice of law: Legal practices in the EU, US and China*, Cambridge University Press, Cambridge, 2010.

Wang Faye Fangfei, *Law of electronic commercial transactions: contemporary issues in the EU, US, and China,* London, Routledge Taylor & Francis Group, 2010.

Warkentin M. (ed), *Business-to-Business Electronic Commerce: Challenges and Solutions*, Hershey, Idea Group Publishing, 2002.

Watson Richard T. et al., *Electronic Commerce: The Strategic Perspective*, Zurich, The Global Text, 2008.

Westland Christopher J. & Theodore H. K. Clark, *Global Electronic Commerce: Theory and Case Studies,* Cambridge, MIT Press, 2000.

Yu Chien-Chih, 'Service-Oriented Data and Process Models for Personalization and Collaboration' in e-Business, in K. Bauknecht et al. (Eds.), *E-Commerce and Web Technologies 2006*, LNCS 4082, Berlin Heidelberg, Springer-Verlag, 2006.

Yuthayotin Sutatip, *Access to Justice in Transnational B2C E-Commerce A Multidimensional Analysis of Consumer Protection Mechanisms*, Switzerland, Springer, 2015.

Zanfir Gabriela, ‘Tracing the Right to Be Forgotten in the Short History of Data Protection Law: The “New Clothes” of an Old Right’ in S. Gutwirth et al. (eds.), *Reforming European Data Protection Law, Law, Governance and Technology Series 20,* Dordrecht, Springer, 2015.

Zanfir-Fortuna Gabriela ‘Article 15. Right of access by the data subject’ in Christopher Kuner, Lee A. Bygrave and Xe Christopher Docksey, *The EU General Data Protection Regulation (GDPR): A Commentary,* New York, Oxford University Press, 2020.

Zhang Qinghua. ‘Customer Satisfaction in B2C E-Commerce Market’ in W. Du (ed.), *Informatics and Management Science VI, Lecture Notes in Electrical Engineering 209*, London, Springer-Verlag, 2013.

Zheng Qin et al., *E-commerce Strategy,* Hangzhou, Zhejiang University Press, 2014.

Zweigert K. & H. Kötz, *Introduction to Comparative Law,* Oxford, Clarendon Press, 1998.

Journal articles

Alexandra Castańeda et al., ‘Research Report ICTs, data and vulnerable people: a guide for citizens’, *University of the Basque Country (UPV/EHU),* Bilbao, 2021, 11-16.

Andreasen Alan R. et al., ‘The Dissatisfaction and Complaining Behavior of Vulnerable Consumers’ *The Journal of Consumer Satisfaction, Dissatisfaction and Complaining Behavior,* 1990, vol.3, 13.

Andrian Rian, Hendradjaya Bayu & Sunindyo Wikan D., ‘Software Assessment Model Using Metrics Products for e-Government in The G2B Model’ 2016 *Fourth International Conference on Information and Communication Technologies (ICoICT),* 2016, 1-2.

Antonella Zarra et al., ‘Sustainability in the Age of Platforms: Final Report’ Brussels, *Centre for European Policy Studies (CEPS*), 2019, 23.

Aulkemeier F. M. et al., ‘A pluggable service platform architecture for e-commerce’ *Information Systems and e-Business Management*, 2015, 9.

Bélanger France & Crossler Robert E., ‘Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems’ *MIS Quarterly,* vol.35/ 4, 2011, 1017-1041.

Bharati Pratyush & Tarasewich Peter, ‘Global Perceptions of Journals Publishing E-Commerce Research’ *Communications of the ACM,* vol.45(5), 2002, 21-26.

Bharosa N. et al., 'Tapping into existing information flows: The transformation to compliance by design in business-to-government information exchange' *Government Information Quarterly,* vol. 30, 2013, 9–18.

Blume Peter, 'The Data Subject', *European Data Protection Law Review (EDPL),* vol.1, no.4, 2015, 259.

Boateng Richard & Hinson Robert, 'E-commerce and socio-economic development; Conceptualizing the link' *Article in Internet Research,* 2008, 564.

Bowen Glenn A., 'Document Analysis as a Qualitative Research Method' *Qualitative Research Journal,* vol.9, no.2, 2009, 27-32.

Breuer Jonas et al., 'Data protection as privilege: Factors to increase meaning of GDPR in vulnerable groups', *Frontiers in Sustainable Cities,* vol.4, 2022, 03.

Bryman Alan, 'The Research Question in Social Research: What is its Role?' *International Journal of Social Research Methodology*, vol/10:1, 2007, 5-20.

Burden Ramil, 'Vulnerable consumer groups: quantification and analysis' *OFT Research paper,* vol.15, 1998, 61.

Butter Den F.A.G. et al., 'Using IT to engender trust in government-to-business relationships: The Authorized Economic Operator (AEO) as an example' *Government Information Quarterly,* vol.29, 2012, 261-274.

Calo Ryan, 'Privacy, Vulnerability, and Affordance', *DePaul L.aw Review,* vol.66, 2017, 592-594.

Cao Y.Z. et al., 'The effects of differences between E-commerce and M-commerce on the consumers' usage transfer from online to mobile channel' *International Journal of Mobile Communications,* 2015, 54.

Cartwright Peter, 'Understanding and protecting vulnerable financial consumers' *Journal of Consumer Policy,* vol:38(2), 2015, 119-138.

Chang Y.F. et al., 'Smart phone for mobile commerce' *Computer Standards & Interfaces,* vol.31, 2009, 740–747.

Colecchia Alessandra, 'Defining and measuring e-commerce: A status Report' *OECD Working papers,* Paris, vol.7, No.78, 1999, 9.

Coltman T. et al, 'E-Business: Revolution, Evolution, or Hype?*' California Management review,* vol.44, No.1, 2001, 59.

Cseres Kati J., 'The Controversies of the Consumer Welfare Standard' *The Competition Law Review,* vol.3/2, 121-173.

De Hert Paul & Vagelis Papakonstantinou, 'The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition' *Computer Law & Security Review,* vol.30, 2014, 633-642.

Duch-Brown Néstor and Martens Bertin, 'Institute for Prospective Technological Studies Digital Economy Working Paper' (2015-07): Barriers to Cross-border eCommerce in the EU Digital Single Market, European Commission, *Joint Research Centre*, 2015, 33-34.

Fineman Martha Albertson, 'The vulnerable subject: Anchoring equality in the human condition' *Yale Journal of Law & Feminism*, vol.20:1, 2008, 8.

Fuster Gloria González, 'How Uninformed is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection', *Revista de Internet: Derecho y Política*, vol.19, 2014, 99.

Gennet et al., 'Does the new EU Regulation on clinical trials adequately protect vulnerable research participants?' *Health Policy*, vol.119, 2015, 925–931.

Goldfarb Avi & Tucker Catherine, 'Why Managing Consumer Privacy Can Be an Opportunity' *MIT Sloan Management Review,* Special Collection: The Fine Line Between Service and Privacy, 2017, 1-3.

Goldfarb Avi & Tucker Catherine, 'Why Managing Consumer Privacy Can Be an Opportunity', *MIT Sloan Management Review*, Special Collection: The Fine Line Between Service and Privacy, 2017, 1-3.

Griffiths Merlyn & Harmon-Kizer Tracy, 'Aging Consumer Vulnerabilities Influencing Factors of Acquiescence to Informed Consent' *Journal of Consumer Affairs*, vol.45/3, 2011, 445-466.

Helberger Natali et al., 'The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law' *Common Market Law Review,* vol.54/5, 2017, 1-2.

Hong I.B. & Cho H., 'The impact of consumer trust on attitudinal loyalty and purchase intentions in B2C e-marketplaces: Intermediary trust vs. seller trust' *International Journal of Information Management*, vol.31, 2011, 469-479.

Huang C. C. et al., 'The agent-based negotiation process for B2C e-*commerce' Expert Systems with Applications,* vol.37, 2010, 348-359.

Huang Z. & M. Benyoucef, 'From e-commerce to social commerce: A close look at design features' *Electronic Commerce Research and Applications,* vol. 12, 2013, 246-259.

Hui Li & Zhao Narisa, 'Better Earlier than Longer: First-Mover Advantage in Social Commerce Product' *Information Competition, Sustainability,* vol.11, 2019, 1-2.

Iankova S. et al., 'A comparison of social media marketing between B2B, B2C and mixed business models' *Industrial Marketing Management,* vol.81, 2019, 169-179.

Kearns Thomas B., 'Technology and the Right to Privacy: The Convergence of Surveillance and Information Privacy Concerns' *William & Mary Bill of Rights Journal*, 1999, 975-976.

Lee S. et al., 'An Analysis of Diversity in Electronic Commerce Research' *International Journal of Electronic Commerce,* vol.12(1), 2007, 31-67.

Lemma Alberto F., 'E-commerce: The implications of current WTO negotiations for economic transformation in developing countries' *Supporting Economic Transformation,* 2017, 13.

Luna Florencia, 'Elucidating the Concept of Vulnerability: Layers Not Labels', *International Journal of Feminist Approaches to Bioethics*, vol.2, 2009, 121.

Mak Vanessa, The 'Average Consumer' of EU Law in Domestic Litigation: Examples from Consumer Credit and Investment Cases, *Legal Studies Research Paper Series*, No. 004/2012, Tilburg Law School, 2012, 4-10.

Malgieri Gianclaudio & Fuster Gloria Gonzalez, 'The vulnerable data subject: A gendered data subject?' *European Journal of Law and Technology,* vol 13(2), 2022, 1-26.

Malgieri Gianclaudio & Niklas Jedrzej 'Vulnerable data subjects', *Computer Law & Security Review,* vol.37, 2020, 105415, 2.

Martens Bertin & Duch Brown Nestor, 'The economics of business-to-government data sharing' JRC Digital Economy Working Paper, No. 2020-04, Seville, European Commission, *Joint Research Centre (JRC),* 2020, 8.

Meire M. et al., 'The added value of social media data in B2B customer acquisition systems: A real-life experiment' *Decision Support Systems,* vol. 104, 2017, 26–37.

Miriyeva Narmin 'European Payments in the Digital Age', ELTE Law Journal, Eötvös University Press, 2022/2, 45.

Mulder Jule, ‘Comparing Vulnerability? How can EU comparative law methods shed light on the concept of the vulnerable consumer’ *Journal of International and Comparative Law (JICL),* vol.6(2), 2019, 209–231.

Neely Phillip R., ‘The Impact and Implementation of E-Commerce in Government & Law Enforcement’ *Journal of Management Policy and Practice* vol.15(1), 2014, 95-97.

Ngai E.W.T. & F.K.T. Wat, ‘A literature review and classification of electronic commerce research’ *Information & Management,* vol.39, 2002, 415-429.

Panayiotou N.A. & Stavrou V.P., ‘Government to business e-services - A systematic literature review’ *Government Information Quarterly,* vol. 38, 2021, 1-2.

Papakonstantinou Vagelis, ‘Cybersecurity as praxis and as a state: The EU law path towards an acknowledgement of a new right to cybersecurity?’ Computer Law & Security Review, vol.44, 2022, 105653, 7.

Pérez María Irigoyen, ‘Report on a strategy for strengthening the rights of vulnerable consumers’ *Committee on the Internal Market and Consumer Protection,* European Parliament 2009-2014: Plenary sitting, A7-0155/2012, 8.5.2012, 6/15.

Poullet Yves, ‘Is the general data protection regulation the solution?’ *Computer law & Security review,* vol.34, 2018, 773-778.

Rahman K. M., ‘A Narrative Literature Review and E-commerce Website research’ *EAI Endorsed Transactions on Scalable Information Systems,* vol.5/17, 2018, 1.

Reitz J. C., ‘How to Do Comparative Law,’ *The American Journal of Comparative Law,* vol.46/4, 1998, 620.

Renda Andrea, ‘Beyond the Brussels Effect,’ FEPS, Belgium, Policy Brief, 2022, 4.

Rhoen Michiel, ‘Beyond consent: improving data protection through consumer protection law’, *Internet Policy Review,* vol.5/1, 2016, 6-8

Šajn Nikolina ‘Vulnerable Consumers Summary’ *EPRS/European Parliamentary Research Service,* 2021, 3.

Šajn Nikolina, ‘New consumer agenda: Summary’ *EPRS/ European Parliamentary Research Service*, Members’ Research Service, PE 679.079, 2021, 1.

Shaw M.J. et al., ‘Research opportunities in electronic commerce’ *Decision Support Systems,* vol.21, 1997, 149-156.

Smith Rhys & Shao Jianhua, 'Privacy and e-commerce: a consumer-centric perspective' *Electron Commerce Research*, 2007, vol.7, 101.

Sohn J. W. & Kim J. K., 'Factors that influence purchase intentions in social commerce' *Technology in Society*, vol.63, 2020, 1-2.

Stănescu Cătălin Gabriel, The Responsible Consumer in the Digital Age: On the Conceptual Shift from 'Average' to 'Responsible' Consumer and the Inadequacy of the 'Information Paradigm' in Consumer Financial Protection, *Tilburg Law Review*, vol.24(1), 2019, 53.

Stoica Eduard & Brote Ioan Victor, 'New technologies shaping the e-commerce environment, Marketing, commerce and Tourism and a New Paradigm of Change' *Revista Economica, Suplimen* nr.3/2012, 383.

Swani K. et al., 'Should tweets differ for B2B and B2C? An analysis of Fortune 500 companies' Twitter communications' *Industrial Marketing Management*, vol.43, 2014, 873-881.

Tzanou Maria, 'Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right' *International Data Privacy Law*, 2013, vol.3/2, 88-89.

Urbaczewski Andrew, Leonard M. Jessup & Bradley Wheeler, 'Electronic Commerce Research: A Taxonomy and Synthesis' *Journal of Organizational Computing and Electronic Commerce*, 2002, vol.12:4, 266-267.

Van Hoecke, M. 'Methodology of comparative legal research' *Law and Method*, 2015, 9.

Webster Jane & Waston Richard T. 'Analyzing the past to prepare for the future: Writing a literature review', *MIS Quarterly*, vol.26, No.2, 2002, xiii.

Wigand Rolf T., 'Electronic Commerce: Definition, Theory, and Context' *The Information Society*, vol.13:1, 1997, 5.

Yoo B., V. Choudhary & T. Mukhopadhyay, 'A model of neutral B2B intermediaries' *Journal of MIS*, vol.19(3), 2003, 43-68.

Zhou L. et al., 'Perceived information transparency in B2C e-commerce: An empirical investigation' *Information and Management*, vol.55, 2018, 912-927.

Zou Y. et al., 'Improving the usability of e-commerce applications using business processes' *IEEE Transactions on Software Engineering*, vol.33, no.12, 2007, 1.

Zwass Vladimir, 'Electronic Commerce and Organizational Innovation: Aspects and Opportunities' *International Journal of Electronic Commerce*, vol.7, no.3, 2003, 7-37.

Zwass Vladimir, 'Electronic Commerce: Structures and Issues' *International Journal of Electronic Commerce*, 1996, vol.1:1, 3.

EU treaties, regulations and directives

Charter of Fundamental Rights of the European Union OJ C 326, 26.10.2012, p. 391–407, Art.38.

Consolidated Version of the Treaty on European Union OJ C 326, 26.10.2012, Art.13.

Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, 47–390.

Council Directive 84/450/EEC of 10 September 1984 relating to the approximation of the laws, regulations and administrative provisions of the Member States concerning misleading advertising OJL 250, 19.9.1984, 17-20.

Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts OJ L 95, 21.4.1993, 29–34.

Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (Text with EEA relevance), PE/50/2022/REV/1, OJL 323, 19.12.2022, 4–26.

Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification) (Text with EEA relevance), OJ L 241, 17.9.2015, 1–15.

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), OJL 337, 23.12.2015, 35–127.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJL 194, 19.7.2016, 1-30.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJL 194, 19.7.2016, 1-30.
Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJL 119, 4.5.2016, 89-131.
Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules (Text with EEA relevance), PE/83/2019/REV/1, OJ L 328, 18.12.2019, 7–28.
Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (Text with EEA relevance.), PE/26/2019/REV/1, OJL 136, 22.5.2019, 1–27.
Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC (Text with EEA relevance.), PE/27/2019/REV/1, OJ L 136, 22.5.2019, 28–50.
Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (Text with EEA relevance) OJ L 409, 4.12.2020, 1-27.
Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance), PE/32/2022/REV/2, OJ L 333, 27.12.2022, 80–152.
Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’), OJ L 178, 17.7.2000, 1–16.

Directive 2000/35/EC of the European Parliament and of the Council of 29 June 2000 on combating late payment in commercial transactions, OJ L 200, 8.8.2000, 35–38.
Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (Text with EEA relevance), OJ L 11, 15.1.2002, 4–17.
Directive 2002/58/EC of The European Parliament and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, 37-47.
Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC OJ L 271, 9.10.2002, 16–24.
Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (Text with EEA relevance) OJ L 149, 11.6.2005, 22–39.
Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising (codified version) (Text with EEA relevance) OJL 376, 27.12.2006, 21–27.
Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests (Codified version) Text with EEA relevance OJ L 110, 1.5.2009, 30-36.
Directive 2011/7/EU of the European Parliament and of the Council of 16 February 2011 on combating late payment in commercial transactions Text with EEA relevance OJ L 48, 23.2.2011, 1–10.
Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance OJ L 304, 22.11.2011, 64–88.

Directive 2014/54/EU of the European Parliament and of the Council of 16 April 2014 on measures facilitating the exercise of rights conferred on workers in the context of freedom of movement for workers Text with EEA relevance, OJ L 128, 30.4.2014, Rec.5, 8–14.
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, 31–50.
Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, OJ L 144, 4.6.1997, 19–27.
Directive 98/27/EC of the European Parliament and of the Council of 19 May 1998 on injunctions for the protection of consumers' interests, OJ L 166, 11.6.1998, 51–55.
Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of the prices of products offered to consumers OJ L 80, 18.3.1998, 27-31.
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, 1–88.
Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, PE/31/2018/REV/1, OJ L 295, 21.11.2018, 39-98.
Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC (Text with EEA relevance.) OJ L 60I, 2.3.2018, 1–15.
Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (Text with EEA relevance) PE/56/2019/REV/1 OJ L 186, 11.7.2019, 57–79.

Regulation (EU) 2019/881 of the European Parliament and Of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance), PE/86/2018/REV/1, OJL 151, 7.6.2019, 15–69.

Regulation (EU) 2021/690 of The European Parliament and Of The Council of 28 April 2021 establishing a programme for the internal market, competitiveness of enterprises, including small and medium-sized enterprises, the area of plants, animals, food and feed, and European statistics (Single Market Programme) and repealing Regulations (EU) No 99/2013, (EU) No 1287/2013, (EU) No 254/2014 and (EU) No 652/2014 (Text with EEA relevance), PE/18/2021/INIT, OJ L 153, 3.5.2021, 1–47.

Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (Text with EEA relevance), PE/13/2021/INIT, OJ L 166, 11.5.2021, 1–34.

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance), PE/17/2022/REV/1, OJ L 265, 12.10.2022, 1–66.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance), PE/30/2022/REV/1, OJ L 277, 27.10.2022, 1–102.

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance), PE/85/2021/REV/1, OJ L 152, 3.6.2022, 1–44.

Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR) OJ L 165, 18.6.2013, 1–12.

Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC Text with EEA relevance, OJ L 158, 27.5.2014, 1–76.

Regulation (EU) No 540/2014 of the European Parliament and of the Council of 16 April 2014 on the sound level of motor vehicles and of replacement silencing systems, and amending Directive 2007/46/EC and repealing Directive 70/157/EEC Text with EEA relevance, OJ L 158, 27.5.2014, 131–195.
Treaty of Rome, Treaty Establishing the European Community, 25 March 1957.

EU case law

Belgian Electronic Sorting Technology, C-657/11, Judgment of the Court (Third Chamber), 11 July 2013, para. 39-60.
Canal Digital Danmark, C-611/14, Judgment of the Court (Fifth Chamber) of 26 October 2016, para. 72.
College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer, Judgment of the Court (Third Chamber) of 7 May 2009, Case C-553/07, paras.23, 42-46, 66-70.
Commission v Belgium, C-421/12, Judgment of the Court (Third Chamber), 10 July 2014, para.59.
Europamur Alimentación, C-295/16, Judgment of the Court (Fifth Chamber) of 19 October 2017, para. 43.
Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Judgment of the Court (Grand Chamber), Request for a preliminary ruling from the Audiencia Nacional, Case C-131/12, 13 May 2014, 1-21.
Gut Springenheide and Tusky v Oberkreisdirektor des Kreises Steinfurts, C-210/96, Judgment of the Court (Fifth Chamber) of 16 July 1998, para. 15, 28-30.
Opinion Of Advocate General Jääskinen delivered on Case C-131/12 Google Spain SL Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González, 25 June 2013, para.110-111.
Patrick Breyer v Bundesrepublik Deutschland, Judgment of the Court (Second Chamber) 19 October 2016, Case C-582/14, para.43-46.
Peter Nowak v Data Protection Commissioner, Judgment of the Court (Second Chamber) of 20 December 2017, Case C-434/16, 20.12.2017, para.34.
RL (C-199/19) Judgment of the Court (Ninth Chamber) of 9 July 2020, paras 21-41.

Telekomunikacja Polska, C-522/08, Judgment of the Court (Third Chamber) of 11 March 2010, para. 33.

UPC Magyarország, C-388/13, Judgment of the Court (First Chamber) of 16 April 2015, para. 63.

Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen, Judgment of the Court (Grand Chamber) 9 November 2010, Joined cases C-92/09 and C-93/09, para. 53.

VTB-VAB NV v Total Belgium NV, Joined cases C-261/07 and C-299/07, Judgment of the Court (First Chamber) of 23 April 2009, para. 52-68.

YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S, Judgment of the Court (Third Chamber), 17 July 2014, Joined Cases C-141/12 and C-372/12, paras.20, 46,58-59.

EU guidance and reports

Article 29 Data Protection Working Party (DPWP), 'Opinion 4/2007 on the concept of personal data', 01248/07/EN, WP 136, adopted on 20th June, 6-7.

Article 29 DPWP, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679', adopted on 3 October 2017, as last revised and adopted on 6 February 2018, 17/EN WP251rev.01, 5-6.

Article 29 DPWP, 'Guidelines on consent under Regulation 2016/679', Adopted on 28 November 2017 as last Revised and Adopted on 10 April 2018, 17/EN WP259 rev.01, 3.

Article 29 DPWP, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679', adopted on 4 April 2017, 17/EN/WP 248, 9.

Article 29 DPWP, 'Guidelines on Personal data breach notification under Regulation 2016/679', adopted on 3 October 2017, as last revised and adopted on 6 February 2018, 18/EN/WP250rev.01, 14.

Article 29 DPWP, 'Guidelines on the right to data portability', adopted on 13 December 2016, as last Revised and adopted on 5 April 2017, 16/EN WP 242 rev.01, 4.

Article 29 DPWP, 'Guidelines on transparency under Regulation 2016/679', 17/EN WP260,10.

Article 29 DPWP, ‘Opinion 03/2014 on Personal Data Breach Notification’, adopted on 25 March 2014, 693/14/EN WP 213, 4.
Article 29 DPWP, ‘Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC’, adopted on 9 April 2014, 844/14/EN/WP 217, 41-50.
Commission Notice, ‘Guidance on the interpretation and application of Article 6a of Directive 98/6/EC of the European Parliament and of the Council on consumer protection in the indication of the prices of products offered to consumers (Text with EEA relevance)’ (2021/C 526/02), 5.
Commission Notice, ‘Guidance on the interpretation and application of Directive 2005/29/EC of the European Parliament and of the Council concerning unfair business-to-consumer commercial practices in the internal market (Text with EEA relevance)’ C/2021/9320, OJC 526, 29.12.2021, 1-129.
Commission Notice, ‘Guidance on the interpretation and application of Council Directive 93/13/EEC on unfair terms in consumer contract (Text with EEA relevance)’ OJC 323, 27.9.2019, 4-92.
Commission Notice, ‘Guidelines on ranking transparency pursuant to Regulation (EU) 2019/1150 of the European Parliament and of the Council (2020/C 424/01)’ C/2020/8579, OJ C 424, 8.12.2020, 1–26.
Commission of The European Communities, ‘Communication from The Commission to The Council, The European Parliament, The Economic and Social Committee and The Committee of the Regions, A European Initiative in Electronic Commerce’, Brussels, 16.04.1997, COM (97) 157 final, 3.
Commission of The European Communities, ‘Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive’, /COM/2007/0087 final, 9.
Commission of The European Communities, ‘Report from the Commission First report on the implementation of the Data Protection Directive (95/46/EC)’, Brussels, 15.5.2003 COM (2003) 265 final, 27.
Consultative Assembly, ‘Committee on Science and Technology Sub-Committee, ‘on’-Data Processing Resolution (74) 29 on the protection of the privacy of individuals vis-d-vis

electronic data banks in the public sector, Strasbourg 13 November 1974, AS/Science/Computer (26) 2, 1-5.
Council of Europe Committee of Ministers, 'Resolution (73) 22 on The Protection of the Privacy of Individuals Vis-a-vis electronic data banks in the private sector' 26 September 1973 at the 224th meeting of the Ministers' Deputies), 1-9.
Council of Europe, 'Convention 108 +' Convention for the protection of individuals with regard to the processing of personal data, 2018, 5-16.
Council of Europe, 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data', European Treaty Series - No. 108, Strasbourg, 28.I.1981, 1-9.
Council of Europe, 'Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data', European Treaty Series - No. 108, Strasbourg, 28.I.1981, 1-16.
Court of Justice of the European Union, 'Electronic Commerce and contractual obligations', Research and documentation directorate, 2020, 1.
EPRS, 'The NIS2 Directive A high common level of cybersecurity in the EU', 7.
EPRS/ European Parliamentary Research Service: EU Legislation in Progress briefing, 'The NIS2 Directive A high common level of cybersecurity in the EU', European Union, 2022, 1.
European Commission, ''Proposal for A Regulation of The European Parliament and Of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012 COM (2012) 11 final 2012/0011 (COD), 2.
European Commission, 'A coherent framework for building trust in the Digital Single Market for e-commerce and online services', Commission Communication to The European Parliament, The Council, The Economic and Social Committee and The Committee of The Regions, Brussels, 11.1.2012, COM (2011) 942 final, 3.
European Commission, 'A Digital Single Market Strategy for Europe', COM (2015) 192 final, 3.
European Commission, 'Commission Recommendation (EU) 2017/1584 of 13 September 2017 on a coordinated response to large-scale cybersecurity incidents and crises', C/2017/6100, OJ L 239, 19.9.2017, 1.

European Commission, 'Commission Recommendation of 11 June 2013 on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union Law', OJ L 201, 26.7.2013, 60-65.

European Commission, 'Commission Staff Working Document Accompanying the document Communication from the Commission to the European Parliament and the Council Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, Brussels, 24.6.2020, SWD (2020) 115 final, 20-21.

European Commission, 'Commission Staff Working Document Executive Summary of The Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148', Brussels, 16.12.2020, SWD (2020) 344 final, 1.

European Commission, 'Commission Staff Working Document Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices', Brussels, 4.12.2009 SEC (2009) 1666 final, 1.

European Commission, 'Commission Staff Working Document Guidance on The Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices Accompanying The Document Communication from The Commission to The European Parliament, The Council, The European Economic And Social Committee And The Committee of The Regions A comprehensive approach to stimulating cross-border e-Commerce for Europe's citizens and businesses,' Brussels, 25.5.2016, SWD (2016) 163 final, 43-46.

European Commission, 'Commission Staff Working Document Identifying Europe's recovery needs Accompanying the document Communication from The Commission to The European Parliament, The European Council, The Council, The European Economic and Social Committee and The Committee of The Regions Europe's moment: Repair and Prepare for the Next Generation', Brussels, 27.5.2020, SWD (2020) 98 final, 1-54.

European Commission, 'Commission Staff Working Document Impact Assessment Accompanying the document Proposal for Regulation of The European Parliament and Of

the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)', Brussels, 10.1.2017, SWD (2017) 3 final, Part 2/3, 8.
European Commission, 'Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148', Brussels, 16.12.2020, SWD (2020) 345, final PART 1/3, 9.
European Commission, 'Commission Staff Working Document Report of the Fitness Check', Brussels, 23.5.2017 SWD (2017) 209 final, 4.
European Commission, 'Commission Staff Working Document: A Digital Single Market Strategy for Europe - Analysis and Evidence Accompanying the document, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Single Market Strategy for Europe', Brussels, 6.5.2015, SWD (2015), 100 final, 1.
European Commission, 'Communication from The Commission to The Council and The European Parliament on the implementation of Directive 1998/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of prices of products offered to consumers', Brussels, 21.6.2006 COM (2006) 325 final, 6.
European Commission, 'Communication from The Commission to The European Parliament and The Council New Consumer Agenda Strengthening consumer resilience for sustainable recovery', Brussels, 13.11.2020 COM (2020), 696 final, 16.
European Commission, 'Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions Smart Regulation in the European Union', Brussels, 8.10.2010 COM (2010) 543 final, 1-12.
European Commission, 'Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions EU Regulatory Fitness', Strasbourg, 12.12.2012, COM (2012) 746 final, 1-11.
European Commission, 'Communication from The Commission to The European Parliament, The Council and The European Economic and Social Committee A New Deal for Consumers', COM/2018/0183 final, 3.

European Commission, ‘Communication from The Commission to The European Parliament and The Council New Consumer Agenda Strengthening consumer resilience for sustainable recovery’, COM/2020/696 final, 3.
European Commission, ‘Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions: A comprehensive approach to stimulating cross-border e-Commerce for Europe’s citizens and businesses’, COM/2016/0320 final, 8.
European Commission, ‘Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions Protecting businesses against misleading marketing practices and ensuring effective enforcement’, Brussels, 27.11.2012 COM (2012) 702 final, 2.
European Commission, ‘Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions A Digital Single Market Strategy for Europe’, Brussels, 6.5.2015 COM (2015) 192 final, 8.
European Commission, ‘Communication from The Commission to The European Parliament, The Council, The Economic and Social Committee and The Committee of The Regions: A comprehensive approach on personal data protection in the European Union’, Brussels, 4.11.2010 COM (2010) 609 final, 1-20.
European Commission, ‘Communication from The Commission to The European Parliament and The Council Data protection rules as a trust-enabler in the EU and beyond – taking stock’, Brussels, 24.7.2019, COM (2019) 374 final, 1.
European Commission, ‘Communication from The Commission to The European Parliament and The Council Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union’, Brussels, 29.5.2019 COM (2019) 250 final, 5-6.
European Commission, ‘Communication from the Commission to The European Parliament and The Council, Data protection as a pillar of citizens’ empowerment and the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation’, Brussels, 24.6.2020, COM (2020) 264 final, 4.
European Commission, ‘Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The

Regions Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry', Brussels, 5.7.2016, COM (2016) 410 final, 2.
European Commission, 'Communication from The Commission to The European Parliament, The European Council, The Council, The European Economic and Social Committee and The Committee of The Regions on the EU Security Union Strategy', Brussels, 24.7.2020, COM (2020) 605 final, 1-28.
European Commission, 'Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions: Shaping Europe's digital future', Brussels, 19.2.2020, COM (2020) 67 final, 1.
European Commission, 'Communication from The Commission to The European Parliament and The Council Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union', Brussels, 4.10.2017, COM (2017) 476 final/2, 2-6.
European Commission, 'Communication from The Commission to The European Parliament, The Council, The Economic and Social Committee and The Committee of The Regions Towards a Single Market Act: For a highly competitive social market economy: 50 proposals for improving our work, business and exchanges with one another', Brussels, 27.10.2010, COM (2010) 608 final, 2.
European Commission, 'Communication from The Commission to The European Parliament, The Council, The Economic and Social Committee and The Committee of The Regions Single Market Act: Twelve levers to boost growth and strengthen confidence 'Working together to create new growth'', Brussels, 13.4.2011 COM (2011) 206 final, 2-4.
European Commission, 'Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions Better Governance for The Single Market', Brussels, 8.6.2012, COM (2012) 259 final, 8-9.
European Commission, 'Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions Upgrading the Single Market: more opportunities for people and business', Brussels, 28.10.2015, COM (2015) 550 final, 3.

European Commission, ‘Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions 2030 Digital Compass: the European way for the Digital Decade’, Brussels, 9.3.2021, COM (2021) 118 final, 1-2.
European Commission, ‘Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions Establishing a European Declaration on Digital rights and principles for the Digital Decade’, Brussels, 26.1.2022, COM (2022) 27 final,1.
European Commission, ‘Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions A European strategy for data’, Brussels, 19.2.2020, COM (2020) 66 final, 1.
European Commission, ‘Communication from The Commission to The European Parliament, The European Council, The Council, The European Economic and Social Committee and The Committee Of The Regions: Artificial Intelligence for Europe Brussels’, Brussels, 25.4.2018, COM (2018) 237 final, 1.
European Commission, ‘Communication from The Commission: Annual Growth Survey 2013’, Brussels, 28.11.2012, COM (2012), 750 final, 8.
European Commission, ‘Consumer vulnerability across key markets in the European Union: Final report’, Luxembourg, Publications Office of the European Union, 2016, 42.
European Commission, ‘Directorate-General for Communications Networks, Content and Technology, Study on Support to the observatory for the online platform economy’: Final report’, Publications Office, 2021, 9.
European Commission, ‘Flash Eurobarometer 443: Briefing note e-Privacy’, 2016, 1.
European Commission, ‘For a highly competitive social market economy: 50 proposals for improving our work, business and exchanges with one another’, COM (2010) 608 final, 4.
European Commission, ‘Green paper on the Review of the Consumer Acquis’, OJC 61, 15.3.2007, 1–23.
European Commission, ‘Joint Communication to The European Parliament and The Council the EU’s Cybersecurity Strategy for the Digital Decade, Brussels, 16.12.2020, JOIN (2020) 18 final, 1-4

European Commission, ‘Proposal for a Directive of The European Parliament and Of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148’, Brussels, 16.12.2020, COM (2020) 823 final, 2020/0359 (COD), 3.

European Commission, ‘Proposal for a Directive of The European Parliament and Of The Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)’, Brussels, 28.9.2022, COM (2022), 496 final 2022/0303 (COD), 1.

European Commission, ‘Proposal for a Regulation of The European Parliament and Of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)’ Brussels, 10.1.2017, COM (2017) 10 final, 2017/0003 (COD), 2.

European Commission, ‘Proposal for a Regulation of The European Parliament and Of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)’ Brussels, 10.1.2017, COM (2017) 10 final, 2017/0003 (COD), 2-5.

European Commission, ‘Proposal for A Regulation of The European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)’, Brussels, 25.1.2012 COM (2012) 11 final 2012/0011 (COD), 2.

European Commission, ‘Proposal for a Regulation of The European Parliament and Of The Council on harmonised rules on fair access to and use of data (Data Act)’, Brussels, 23.2.2022, COM (2022), 68 final 2022/0047 (COD), 2.

European Commission, ‘Proposal for a Regulation of The European Parliament and of The Council on contestable and fair markets in the digital sector (Digital Markets Act)’, Brussels, 15.12.2020, COM (2020), 842 final, 2020/0374 (COD), 3.

European Commission, ‘Proposal for a Regulation of The European Parliament and Of The Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC’, Brussels, 15.12.2020, COM (2020), 825 final, 2020/0361 (COD), 1-2.

European Commission, 'Proposal for a Regulation of The European Parliament and of The Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts', Brussels, 21.4.2021, COM/2021/206 final, 1-3.
European Commission, 'Proposal on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148', COM (2020) 823 final, 2020/0359 (COD), 1.
European Commission, 'Report from The Commission concerning the application of Directive 98/27/EC of the European Parliament and of the Council on injunctions for the protection of consumers' interest', Brussels, 18.11.2008 COM (2008) 756 final, 5.
European Commission, 'Report From The Commission To The European Parliament, The Council And The European Economic And Social Committee First Report on the application of Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive')' Brussels, 14.3.2013 COM (2013) 139 final, 2.
European Commission, 'Report from The Commission to The European Parliament and The Council Concerning the application of Directive 2009/22/EC of the European Parliament and of the Council on injunctions for the protection of consumers' interest', Brussels, 6.11.2012 COM (2012) 635 final, 7.
European Commission, 'Report from The Commission to The European Parliament and The Council on the implementation of Directive 2011/7/EU of the European Parliament and of the Council of 16 February 2011 on combating late payment in commercial transactions' {SWD (2016) 278 final}, 9.
European Commission, 'Report from the Commission to the European Parliament, the Council and the Economic and Social Committee on the safety and liability implications of artificial intelligence, the internet of things and robotics', Brussels, 19.2.2020, COM (2020) 64 final, 1.
European Commission, 'Synopsis Report of The Public Consultation on The Evaluation and Review of the e-Privacy Directive', 2016, 2-3.

European Commission, ‘the EU’s approach to the digital transition - two years of application of the General Data Protection Regulation’, COM (2020) 264 final, 7.
European Commission, ‘the EU’s Cybersecurity Strategy for the Digital Decade’, JOIN (2020) 18 final, 1-29.
European Commission, Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions Single Market Act II Together for new growth (Text with EEA relevance), Brussels, 3.10.2012, COM (2012) 573 final, 4.
European Commission, Directorate-General for Justice and Consumers, ‘How does the data protection reform strengthen citizens’ rights?’ Publications Office, Factsheet, 2018.
European Commission, Directorate-General for Justice and Consumers ‘Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation’ *Final Report*, Brussels, 2022, 91-109.
European Commission, European Declaration on Digital Rights and Principles for the Digital Decade Brussels, 26.1.2022, COM (2022) 28 final, 1.
European Construction Sector Observatory, ‘Late payment in the construction sector’, Analytical Report, 2020, 8-9.
European Data Protection Supervisor, ‘Preliminary Opinion of the European Data Protection Supervisor, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy’, Brussels, 2014, 3.
European Union Agency for Fundamental Rights and Council of Europe, ‘Handbook on European data protection law 2018 edition’, Publications Office of the European Union, Luxembourg, 2018, 34.
European Union Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law 2018 edition’, 205.
European Union Global Strategy, ‘A Global Strategy for the European Union’s Foreign and Security Policy: ‘Shared Vision, Common Action: A Stronger Europe,’’ 2016, 1-60.

Miscellaneous

Bram Benjamin Duivenvoorde, 'The consumer benchmarks in the Unfair Commercial Practices Directive Thesis', *Digital Academic Repository*, Universiteit van Amsterdam, 2014, 67-68.

IT Governance Privacy Team, 'EU General Data Protection Regulation (GDPR) An implementation and compliance guide', UK, IT Governance Publishing Ltd, 2020, 63.

Other reports and recommendations

BEUC: The European Consumer Organisation, 'Towards European Digital fairness: BEUC framing response paper for the REFIT consultation', Brussels, 20/02/2023, 4.

Civic Consulting, 'Study for the Fitness Check of EU consumer and marketing law', Final report Part 1 – Main report, Brussels, European Commission, 2017, 43-44.

Commission for Customers in Vulnerable Circumstances, 'Final Report 2019', 2019, 19-20.

Directorate for Financial and Enterprise Affairs Competition Committee: Cancels & replaces the same document of 4 May 2018, 'Implications of E-commerce for Competition Policy', Background Note, DAF/COMP (2018)3, 5.

E-commerce Europe, 'Policy recommendations on the role of online platforms in the e-commerce sector', Brussels, 2016, 3-6.

Financial Conduct Authority, Occasional Paper No 8: Consumer Vulnerability, London, 2015, 6-8.

International Trade Centre, 'Bringing SMEs onto the e-Commerce Highway', *ITC*, Geneva, 2016, 11.

McKinsey & Company, 'Future of retail operations: Winning in a digital era', Issue 2, McKinsey & Company, 2020, 4-9.

OECD, 'A Roadmap Toward A Common Framework for Measuring The Digital Economy: Report for the G20 Digital Economy Task Force', Saudi Arabia, 2020, 28.

OECD, 'Electronic and Mobile Commerce', OECD Digital Economy Papers, No. 228, Paris, OECD Publishing, 2013, 7-13.

OECD, 'Measuring the Digital Transformation: A Roadmap for the Future', Paris, OECD Publishing, 2019, 575.

OECD, 'OECD Guide to Measuring the Information Society', Paris, OECD Publishing, 2011, 73.

OECD, ‘OECD Internet Economy Outlook 2012’, Paris, OECD Publishing, 2012, 289-290.
OECD, ‘Sacher Report’, OECD Digital Economy Papers, No. 29, Paris, OECD Publishing, 1997, 20.
OECD, ‘The E-Government Imperative’, OECD Journal on Budgeting, Paris, OECD Publishing, vol.3(1), 2003, 83.
OECD, ‘The Internet Economy on the Rise: Progress since the Seoul Declaration’, Paris, OECD Publishing, 2013, 125.
OECD, ‘Toolkit for Protecting Digital Consumers: A Resource for G20 Policy Makers’, Buenos Aires, OECD, 2018, 8.
OECD, ‘Unpacking E-Commerce: Business Models, Trends and Policies’, Paris, OECD Publishing, 2019, 32.
Ovum Report, ‘The Future of E-commerce: The Road to 2026,’ 2017, 12.
UN ESCAP, ‘Selected issues in cross-border e-commerce development in Asia and the Pacific’, Studies in Trade, Investment and Innovation No. 91, United Nations publication, 2019, 4-5.
UNCTAD, ‘Information Economy Report 2005’, New York, United Nations, 2005, 90.
UNCTAD, ‘Information Economy report 2015: Unlocking the potential of E-Commerce for developing countries’, Geneva, UNCTAD Research Papers, 2015, 3.
UNCTAD, ‘Information Economy report 2015’, New York, United Nations, 2015, 4.
UNCTAD, ‘What Is at Stake for Developing Countries in Trade Negotiations on E-Commerce? The Case of the Joint Statement initiative’ UNCTAD Research Paper, 2021, v.
United Nations Commission on International Trade Law, ‘UNCITRAL Model Law on Electronic Commerce, with Guide to Enactment 1996: with Additional Article 5 bis as Adopted in 1998’, New York, United Nations, 1999, 1-17.
United Nations Industrial Development Organization (UNIDO), ‘BRICS Plus E-commerce Development Report in 2018’, 2019, 12-13.
United Nations, ‘United Nations Economic Commission for Europe: The Impact of Globalization on National Accounts’. New York, United Nations, 2011, 250.
World Customs Organization, ‘WCO Study Report on Cross-border E-commerce’, 2017, 7.
WTO, ‘Declaration on Global Electronic Commerce’, Geneva WTO Ministerial 1998: Electronic Commerce, T/Min (98)/Dec/2, 20 May 1998, 1.

WTO, ‘E-commerce in Developing Countries Opportunities and challenges for small and medium-sized enterprises’, Geneva: World Trade Organisation, 2013, 2.
WTO, ‘Joint Statement on Electronic Commerce’, WT/L/1056 25 January 2019 (19-0423), 1/1.
WTO, ‘Ministerial Conference Eleventh Session Buenos Aires: Joint Statement on Electronic Commerce’, WT/MIN (17)/60, 13 December 2017 (17-6874), 1/1.

Online sources

Digital fairness - fitness check on EU consumer law < https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_enlast> accessed 23 Aug. 2023.
European Commission, The Digital Services Act package < https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package > accessed 27 Aug. 2023.
European Council of the European Union, ‘A new strategic agenda for the EU 2019-2024’, <https://www.consilium.europa.eu/en/eu-strategic-agenda-2019-2024/> accessed 05 Aug. 2023.
Florian Dietrich & Dr. Reemt Matthiesen, CMS: e-Privacy European Regulation on Privacy and Electronic Communications, < https://cms.law/en/deu/insight/e-privacy> accessed 20 Aug. 2023.
Gianclaudio Malgieri & Antonio Davola, Data-Powerful, February 5, 2022, 1-3. <https://ssrn.com/abstract=4027370 > accessed 15 Aug. 2023.
History of the EU: Pioneers, <https://european-union.europa.eu/principles-countries-history/history-eu_en > accessed 15 Aug. 2023.
Platform-to-business trading practices, <https://digital-strategy.ec.europa.eu/en/policies/platform-business-trading-practices> accessed 08 Aug. 2023.
Regulatory framework proposal on artificial intelligence < https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai > accessed 10 Aug. 2023.
Sources of the European Union law, < https://eur-lex.europa.eu/EN/legal-content/summary/sources-of-european-union-law.html > accessed 03 Aug. 2023.