CZĘŚĆ I
Problemy cyberbezpieczeństwa w wymiarze międzynarodowym

Wojciech Rafał Wiewiórowski

Rozdział 1.
Protection of Personal Data in the Year of the Pandemic

1. Introduction

The COVID-19 pandemic has made the daily lives of Europeans more dependent on the proper use of the digital environment. It has accelerated the implementation of new technologies supporting the digital transformation, which became a prerequisite for combating the effects of the pandemic. In 2020, the inhabitants of countries highly developed in terms of economics, realized how dependent they are on digital services at work, when interacting with public administration, and in all aspects of their everyday life. A direct consequence of this situation was the unprecedented increase in personal data processing and the development of new forms of digital communication interfering with the privacy of users. The question of how much it would cost for members of the society to give up some of their rights and freedoms linked to the protection of personal data and privacy of individuals, in order to combat the difficult circumstances they have found themselves in, has ceased to be a philosophical issue and has become a daily dilemma, in view of the continuously increasing number of cybersecurity incidents and personal data breaches[1].

The pandemic has served as a magnifying glass for global trends that pervade our societies: wealth distribution inequalities, exploitation of the most vulnerable, discrimination and social justice outrage. Much of it was predictable, but we should not treat it as a reason to lower our guard. The pandemic-related risks constitute the perfect opportunity for some to exploit perhaps the most sensitive personal data – information concerning one's health[2]. Already at the beginning of 2020, concerns were voiced in regard to how corporate en-

[1] *W. Wiewiorowski*, Projecting Privacy and Data Protection in a Responsible, Sustainable Future, p. 253–258.
[2] *J. Berenger*, Medical Information Systems Ethics, p. 5–7.

tities were appropriating health data for purposes covered by business secrecy. The Pandora's box has now been opened, with digital behemoths conquering the almost unexplored and virgin – at least until now – world of health data markets. In the past year, big tech companies whose business model is based on the exploitation of personal data, have seen their profits increase, while economies worldwide were severely shrinking[3].

Europeans have realized that processing huge amounts of information in the big data world is not a future challenge for the world of the Internet of Things and it will not occur in practice in our everyday life until the number of devices connected to the Internet increases by at least an order of magnitude. It suddenly turned out that we have to 'digitize' as many of our activities as possible already today; whether we like it or not, we are becoming more and more dependent on the Internet connection at work, at school, and at home.

2. Digital solidarity

The development of the Covid-19 crisis has resulted in an increased collection of patients' data. The same, however, concerned also consumers' data, since commercial services needed to be provided online – due to their physical locations being closed. Similar phenomena took place in other areas of people's lives, such as education, work, and social relations. The crisis of 2020 affected everyone, but the biggest consequences were suffered by the weakest and the most vulnerable. Matching personal data obtained from different sources and reusing the digital footprints that we generate every day can potentially lead to the disappearance of, or at least to bypassing the safeguards created by law. This new reality requires the entities responsible for data protection to remain committed to striking the right balance between the need for public health and the protection of privacy and personal data.

It also creates a need for a kind of digital solidarity, which would ensure that data and technologies work for humankind, in accordance with the requirements of GDPR[4], and, in particular, for the most vulnerable[5]. A reformed European data protection system is intended to be part of the EU's economic recovery, as the right to the protection of personal data is based on the value of human dignity and on informational self-determination[6]. This reformed legal system should, at the same time, become a factor enabling people to live freely

[3] *M. Ebeling*, Healthcare and Big Data, p. 98–100.

[4] 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), OJ 2016 L 119/1, p. 1–88 (GDPR), recital 4.

[5] The Europen Data Protection Supervisor, Shaping a Safer Digital Future: a new Strategy for a new decade – EDPS Strategy 2020–2024, Brussels 2020, https://edps.europa.eu/sites/edp/files/publication/20-06-30_edps_shaping_safer_digital_future_en.pdf (access: 11.1.2021).

[6] *M. Koning*, The purpose, p. 72–74.

within a society and to strengthen the economic foundations of that society. Digital solidarity as one of the guiding principles of post-COVID economic recovery will not allow for duplication of business models of continuous surveillance and tracking that destroy confidence in a digital society. Solidarity is also of obvious historical importance, as the idea of rebuilding the world through the joint effort of all social groups mimics what has already happened in Poland in 1980s and 1990s.

3. European Data Spaces

When shaping the vision of the Next Generation Europe Next Generation Europe[7], the European Commission has decided to build on previous strategies and actively support the creation of common European data spaces – understood as spaces for the storage of personal data in such a way that processing can take place without the transfer of personal data to third parties. This would ensure maximum protection of personal data and privacy. Such 'data cooperatives' are intended to empower individuals to make informed choices and consciously give consent to the use of their data.

The nine proposed spaces are to cover the following types of data[8]:

1) industrial (manufacturing) data – to support the competitiveness and productivity of EU industries and enable the potential use of non-personal data in the manufacturing industry;
2) data on the Green Deal;
3) data on mobility;
4) data on health – essential to making progress in preventing, detecting, and treating diseases, and to making informed, evidence-based decisions to improve the accessibility, effectiveness, and sustainability of healthcare systems;
5) financial data;
6) data concerning energy;
7) data concerning agriculture;
8) data on public administration – to increase transparency and accountability, as well as the quality of public spending, to fight corruption more effectively, both at the EU and at the national level, to meet the needs of law enforcement agencies and to support the effective application of EU law and enable the implementation of innovative solutions in the areas of 'govtech', 'reg-tech' and 'legal-tech' as well as other services of public interest;
9) data on skills.

[7] European Commission, Shaping Europe's digital future, Luxemburg 2020.
[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: A European strategy for data, COM(2020) 66 final, p. 23–24.

4. E-health

It has become clear that, out of the current and future applications of big data and artificial intelligence technologies in the healthcare sector, e-health is especially fundamental to further development of industry and science[9]. The need to improve the accessibility, effectiveness and sustainability of e-health systems in the European Union has been highlighted by the particular effort made in the fight against SARS-CoV-2 in the field of scientific research on containing the pandemic and coming up with pharmaceutical responses to it.

Public health policy is an area where citizens of the EU should benefit from the increasingly high quality of healthcare, with growing opportunities to conduct research and reduced costs of obtaining the relevant services. As a result, the medical community and politicians in charge of public health administrations could make informed decisions based on proven evidence from current sources. However, the above is not possible without ensuring the cybersecurity of the health sector, science, and public sphere. A significant step in ensuring such security consists in enabling efficient processing of personal data, as well as protection of the rights and freedoms associated with it[10]. Therefore, one of the main messages that data protection authorities emphasized in their fight against the pandemic, was that we should not be protecting 'data', but – first and foremost – people. Effective processing of personal data should allow us to work to the benefit of humanity, without harming the individual data subjects.

At the same time, the European Commission has taken active steps to create the legal and organizational basis for such a pan-European approach to data processing with social benefits. The digital service infrastructure for e-health (eHDSI) supported by the Commission has been developed, in order to facilitate the interoperability of services offered by Member States. The Commission intends to create a European data space, which should guarantee availability of large-scale data resources, as well as provide the tools and technical infrastructure necessary for the use and exchange of data. Such data space should be complemented by policies intended to stimulate data use and demand for data-enriched services.

5. The special position of research during the Covid-19 crisis

The condition *sine qua non* for creating a common data space system is the availability of large-scale data resources and coming to a broad consensus on the use of personal and non-personal data in scientific research. Such a consensus should include a harmonious interpretation of the GDPR, while

[9] *W. Lowrance*, Privacy, Confidentiality, p. 10–11.
[10] *T. Godlove*, Guide to Healthcare Information Protection, p. 11–13 and 66–114.

bearing in mind that scientific research enjoys a privileged position in the Regulation. The GDPR adopts a relatively liberal approach to the processing of personal data within the framework of scientific research, in order to support innovation and to constantly remind Europeans that science is a public good and a key priority for the entire European Union.

The GDPR provides for the possibility to be exempt from some of the more rigid rules in terms of limiting the purpose of processing[11], if said purpose falls within the concept of scientific research[12]. This means, inter alia, that scientists may use certain data for purposes other than the ones for which they had initially collected it. However, this flexibility remains in line with the Charter of Fundamental Rights, and research and innovation cannot justify an overly liberal interpretation of exemptions that violate the 'essence'[13] of personal data protection as a fundamental right. Under such circumstances, it is important to coordinate the specific rules that Member States may create themselves by introducing specific conditions and new restrictions on the processing of genetic[14], biometric[15] or health data[16], as it creates a risk of fragmentation and may subsequently hinder the flow of personal data within the common European space.

While the aim of such a liberal approach to data processing for the purpose of research is aimed at promoting the secondary use of research results, concerns arise when the roles and responsibilities of researchers change along with the changing purpose of data processing. The same research center may turn from a data processor into a data controller[17] or from a joint-controller into one acting independently[18]. It may also suddenly realize that a previously unknown entity was performing the research for another purpose and become a joint-controller of a resource over which the original controller used to have full control. The role of a person who is a scientist, a practitioner (e.g. a surgeon), a lecturer, a dean or perhaps an employee (or collaborator) of an external commercial entity, all at the same time (which is not uncommon in some scientific institutions), may also change dynamically. In the context of this important discussion and fundamental initiatives for the cross-border exchange of health data, as well as access to health resources for primary and secondary use, it is important to stress that personal data constitutes a raw contribution to scientific research and therefore it is essential for ensuring quality and reliability in the development of scientific research. We shall also note that the

[11] *M. Koning*, The purpose, p. 189–190.
[12] *W. Svanberg*, in: *C. Kuner*, *C. Docksey*, *L. Bygrave* (ed.), The EU General, p. 1243–1244.
[13] *L. Georgieva*, *C. Kuner*, in: *C. Kuner*, *C. Docksey*, *L. Bygrave* (ed.), The EU General, p. 379.
[14] *T. Godlove*, Guide to Healthcare Information Protection, p. 196–214; *M. Hayry*, *T. Takala*, in: *M. Chadwick*, *R. Arnason* (ed.), American principles, p. 14–36.
[15] *M. Hu*, Biometric Surveillance and Big Data Governance, *M. Hayry at al.*, The Ethics, p. 121–149.
[16] *M. Duerr-Specht*, *R. Goebel*, *A. Holzinger*, Medicine and Health Care as a Data Problem, p. 21–40.
[17] *L. Bygrave*, *L. Tossoni*, in: *C. Kuner*, *C. Docksey*, *L. Bygrave* (ed.), The EU General, p. 145–156.
[18] *B. Van Alsenoy*, Data Protection, p. 566 and 582.

boundary between private sector research and traditional research is becoming increasingly blurred and it is at times difficult to distinguish between research that benefits societies at large and research that serves primarily private interests.

Considering the great importance of genetic, biometric, and all other health-related data in the fight against the Covid-19 pandemic and bearing in mind the potential benefits for mankind, the European Data Protection Board (EDPB[19]) has issued specific guidelines on the processing of health data for research purposes in the context of the Covid-19 outbreak. In the guidelines, the Board referred to the existing doubts about the legal basis for data processing, data protection rules, the information duties towards data subjects, and the international transfer of data[20].

The area where the GDPR offers new opportunities and which is still, in fact, not very well-known, is the standardization of data protection practices[21] in scientific research. The GDPR provides for the development of codes of conduct, binding corporate rules (for global companies involved in research activities) and so-called certification mechanisms. Codes of conduct may be developed by research organizations and health professionals to compliment the application of the GDPR with an added value to the interpretation of the Regulation. It seems particularly useful to adopt such codes of conduct where consenting practices, re-use of personal data and specific appropriate safeguards to be implemented in the course of research are concerned. Some codes are currently under preparation, in particular in the field of biobanks and in the pharmaceutical sector.

All discussions triggered directly by the pandemic coincided with the beginning of regulatory action on Artificial Intelligence in the European Union[22]. 2020 was also the year of European discussions on data governance[23] and the future of the digital services regulation[24]. The European Union decided that, despite the current crisis, it needs to develop and find answers to both

[19] The European Data Protection Board (EDPB) is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU's data protection authorities. The EDPB is composed of representatives of the national data protection authorities, and the European Data Protection Supervisor (EDPS). The supervisory authorities of the EFTA EEA States are also members with regard to the GDPR related matters and without the right to vote and being elected as chair or deputy chairs.

[20] Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf *(*access: 1.2.2021).

[21] *C. Kuner*, European Data Protection Law, p. 39–41.

[22] European Commission, White Paper on Artificial Intelligence: a European approach to excellence and trust, COM(2020)65 final.

[23] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM(2020)767 final.

[24] 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, COM(2020) 825 final.

old and new challenges. At the same time – because of the crisis – it needs to do this more efficiently and more reasonably than it was done so far. Practical solutions linked to the application of Artificial Intelligence technologies play a particularly important role in the field of healthcare[25], as they have the potential to offer a number of direct benefits to researchers, as well as in terms of improving daily patient care, but also in regard to supporting translation services and assisting in the process of making clinical decision[26]. Nevertheless, the dangers linked to misusing them ought not to be forgotten[27].

The European Commission, taking into account the experience gained in connection with the avian flu and Ebola outbreaks in the previous decade, has included in its communication on artificial intelligence references to the role of the practical application of artificial intelligence algorithms in facilitating the digital transition of the healthcare sector into the digital single market. What needs to be borne in mind is that the fact that said communication was presented in February of 2020, and it was prepared before the outbreak of the pandemic.

6. The impact of the crisis on the development of eGovernment services

The crisis has also had a huge impact on the legal and political decisions concerning the application of modern IT and telecommunications solutions by public administration, both at the national and at the European level. However, the observed changes are not limited to legal questions or proposed paths to respond the crisis[28]; they also help in the development of new undertakings and accelerate the speed of transformation. While traditionally the sector of new IT technologies and large-scale information systems made Member States and EU institutions have to carry out long-term pilot projects and perform their multi-directional evaluation before each successive expansion, the 2020 pandemic has posed the question to Member State governments and EU administration whether a pan-European, interoperable project can be launched within a timeframe of weeks. While the administration has always been willing to announce the 'triumph' of its IT projects if at least 10% of citizens used them at least once, in order to achieve success in the fight against COVID-19, 60% of the population will need to be permanently using the newly introduced technical solutions[29].

[25] European Commission, White Paper, p. 2 and 9–10.
[26] *T. Godlove*, Guide to Healthcare Information Protection, p. 13–18.
[27] *S. Russel*, Human Compatible, p. 103–132.
[28] *N. Fabiano*, GDPR & Privacy, p. 245–275.
[29] *W. Wiewiórowski*, Rola Unii Europejskiej, p. 23–30; *L. Ferretti et al.*, Quantifying SARS-CoV-2 transmission, p. 6491; *L. Floridi*, Mind the app.

Since the beginning of the pandemic in the spring of 2020, both the administrations and the citizens of the RU have been well aware that automated data processing and digital technologies can become key elements of the fight against COVID-19. However, they also realized that the effect of such actions will go far beyond the crisis period. This, in turn, means that it is also the duty of the EU institutions to ensure that any measure taken in these extraordinary circumstances is necessary and limited in terms of its duration and scope and that is subject to periodic practical reviews based on a scientific method. Members of the society should not be forced to choose between an effective response to the current crisis on one hand and the protection of their fundamental rights on the other. Both of these goals can be achieved together[30]. EU law allows for the responsible use of data and communication techniques for health management purposes, while ensuring that the process does not restrict the rights and freedoms of individuals.

7. Looking to the future

Although Europe has realized that the data protection reform facilitated the decision-making process during the Covid-19 crisis, with GDPR in place Europe cannot rest on its laurels. The practical implementation of the intentions of the European legislators will continue to be evaluated and any mistake made in the course of the harmonious implementation of the GDPR principles can be used to criticize the protection of personal data as a fundamental right. For the public administration – both at the EU level and in each Member State – to be able to control the growing complexity of digital systems, which may be based on business models relying on data collection by a narrow group of private sector data controllers[31], constitutes the real challenge to be assessed. The new decade will be a time of crusade for control over the so-called industrial data, in which Europe wants to play a leading role. We will certainly witness a proliferation of dynamic systems consisting of interconnected devices. This will increase the risk of systems built for the public sector becoming compromised, allowing external entities to gain access to protected information – including personal data. Ensuring security and fair competition throughout the election processes will become crucial for democracy.

The crisis has highlighted the particular importance of ensuring privacy and personal data protection. However, it is to be expected that during the period of recovery from said crisis, its economic impact will increase the pressure put on organizations to maximize their effectiveness, perhaps with less attention paid to individual rights and freedoms. When responding to this challenge, the entities responsible for data protection should focus on areas where

[30] *L. Odwazny*, Societal Lapses in Protecting Individual Privacy, p. 223–236.
[31] *S. Zuboff*, The Age of Surveillance Capitalism, p. 182.

data protection interacts with technology, and closely monitor all emerging innovations, issuing warnings when technology is implemented in a way that does not respect the essence of fundamental rights to personal data protection.

Public administration in the European Union cannot rely solely on external digital service providers to fulfil its tasks. The EU has the opportunity to bring about real changes in the market and to transform business models that deviate from EU values and laws. The above will be crucial to creating a strong oversight of the technologies and tools that are becoming increasingly 'endemic' to our digital ecosystem.

Celebrating the 40th anniversary of the Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data on January 28th should mark the moment when national supervisory authorities of the European Data Protection Board (EDPB) become involved in fully coordinated – or even joint – enforcement actions under GDPR and the so-called Law Enforcement Directive[32]. They should not, however, miss the great opportunity offered by GDPR. In the upcoming years, the regulation concerning digital services and digital markets should be brought forward, with the intention of tackling the increasing risks for fundamental rights and other societal harms in the digital sphere. Regulators ought to act with the bravery and courage required in these challenging times, as the choices made today will determine the world of tomorrow.

[32] 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, OJ L 119, 4.5.2016, p. 89–131.

Abstract

The COVID-19 pandemic has made the daily lives of Europeans more dependent on proper use of the digital environment. It has accelerated the implementation of new technologies supporting the digital transformation, which became a prerequisite for combating the effects of the pandemic. New reality requires the entities responsible for data protection to strike the right balance between the need for public good and the protection of privacy and personal data. Certain kind of digital solidarity should ensure that data and technologies work for humankind, in accordance with the requirements of the European data protection law. This chapter observes the data protection challenges of common European data spaces envisaged by the European Commission in the Next Generation EU strategy. Such 'data cooperatives' are intended to empower individuals to make informed choices as far as the use of their data for scientific purposes is concerned.

Streszczenie

Pandemia COVID-19 w namacalny sposób uwidoczniła, jak bardzo codzienne życie Europejczyków uzależnione jest od właściwego wykorzystania środowiska cyfrowego. Przyspieszyła również wdrażanie nowych technologii wspierających transformację cyfrową, która stała się warunkiem koniecznym do zwalczania skutków pandemii. Nowa rzeczywistość wymaga od podmiotów odpowiedzialnych za ochronę danych osobowych znalezienia właściwej równowagi pomiędzy działaniami realizowanymi dla dobra publicznego a ochroną prywatności i danych osobowych. Pewien rodzaj cyfrowej solidarności powinien zapewnić, by dane i technologie pracowały na rzecz ludzkości zgodnie z wymogami europejskiego prawa ochrony danych. Niniejszy rozdział poświęcony jest wyzwaniom związanym z ochroną danych w ramach wspólnych europejskich przestrzeni danych, przewidzianych przez Komisję Europejską w strategii Next Generation Europe. Takie „spółdzielnie danych" mają umożliwić osobom fizycznym dokonywanie świadomych wyborów w zakresie wykorzystywania ich danych do celów naukowych.

Justyna Romanowska

Rozdział 2.
A cyberpandemic – EU plans to support cybersecurity in the new multiannual financial perspective 2021–2027

1. Introduction – general overview, timeline, proposed figures, procedural context

The new European Union budget for the next multiannual financial perspective (MFF) proposed in 2018 called the 'EU Budget for the Future' is worth in total €1.1 trillion[1]. In addition to that, in June 2020, the European Commission also proposed the introduction of a new temporary recovery instrument aimed at mobilizing investments and kick-starting the European economy[2]. Said new temporary instrument, called the Next Generation EU, will run from 2021 to 2024 and it is worth €750 billion. It will also feed into some of the digital strands (for example the Invest EU program, Horizon Europe, the Just Transition Fund and others). All this makes the next EU budget very large and complex but also very promising.

An inter institutional agreement between the co-legislators (the Council of the EU and European Parliament) on the revised multiannual financial perspective for 2021–2027 took place in December 2020, with the final step being the consent of the European Parliament given during 14–18 December plenary session. The implementation of the new budget begins in January 2021. In practice, it means that the next step of the European Commission

[1] Communication from the Commisision, A Modern Budget for a Union that Protects, Empowers and Defends. The Multiannual Financial Framework for 2021–2027, COM (2018)321 final https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0321&from=EN (access: 15.2.2021), COM(2018)321 final.

[2] Proposal for a Council Regulation establishing a European Union Recovery Instrument to support the recovery in the aftermath of the COVID-19 pandemic, COM (2020)441 final https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0441R(01)&from=EN (access: 15.2.2021).

should be to adopt shortly the first multiannual work programs for specific sectors of the economy, including digital. These will set out a timetable of calls for proposals for 2021–2023, the topics to be covered, an indicative budget, and a prospective framework for the entire programming period (2021–2027).

Pursuant to Article 312 TFUE, the MFF is being adopted in the form of a regulation in a special legislative procedure, with the Council of the European Union acting unanimously after receiving the consent of the European Parliament, expressed by an absolute majority[3]. Alternatively, the European Council may unanimously authorize the Council to act upon a decision made by a qualified majority when adopting the MFF regulation. Additionally, according to Article 321(5) TFEU, the European Parliament, the Council and the Commission are required to take any measure necessary to facilitate the adoption of the MFF.

On 27 May 2020, in order to support the recovery in the aftermath of the COVID-19 pandemic, the European Commission presented a recovery and resilience package including an amended proposal for the 2021–2027 MFF, an amended proposal for a decision on the system of Own Resources, and a proposal for a regulation establishing an EU recovery instrument (the Next Generation EU) for the years 2021–2024[4]. According to the proposal, the Next Generation EU resources amounting to €750 billion, borrowed on behalf of the EU by the Commission on the financial markets, would top up the 2021–2027 MFF worth €1.1. trillion. Channeled through the already existing MFF and the new programs, the recovery funds would provide support to the EU economy, where it is the most needed. The borrowed funds will, however, be supplementary to the annual budget and they will not be a part of the MFF and of the annual budgeting procedure. The proposed changes concerned the structure and the total size of the MFF, as well and the allocations for individual programs and funds. In particular, the Commission proposed an MFF which is 3% (€34.6 billion) lower than its own proposal from 2018 and reduced the allocations for some programs, such as the Connecting Europe Facility (-8.4%), the European Defense Fund (-30%), the European military mobility (-74%), and Erasmus+ (-6.7%). The use of the resources from the Next Generation EU to reinforce such spending areas as heading 1 'Single market, Innovation and digital' (+€69.8 bln), heading 2 'Cohesion and values' (+€610 bln), heading 3 'Natural resources and environment' (+€45 bln), head-

[3] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union - Consolidated version of the Treaty on the Functioning of the European Union - Protocols - Annexes - Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007 - Tables of equivalences, Official Journal C 326 , 26.10.2012, p. 0001–0390, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012E/TXT.

[4] https://ec.europa.eu/info/strategy/eu-budget/long-term-eu-budget/eu-budget-2021-2027_en#commission-proposal-may-2020 (access: 15.2.2021).

ing 5 'Resilience, security and defense' (+€9.7 bln), and heading 6 'Neighborhood and the world' (+€15.5 bln) was suggested.

2. Digital sector in the new multiannual financial perspective

The objective of the new MFF regarding the digital sector is to ensure that Europe leads the digital transformation of society and economy, bringing benefits to all citizens and businesses. More specifically, new actions regarding the digital sector should focus on: reinforcing the EU's digital capabilities (including cybersecurity, computing, data, artificial intelligence), ensuring their widest possible roll out and maximizing their benefits, preparing for and leading the development of next generation technologies, building a world-leading connectivity infrastructure, as well as supporting creators and ensuring the widespread distribution of their works.

To be able to properly prepare for the absorption of those funds, it is crucial to have clarity as to what the purpose of every financial instrument is and how it can support the development of cybersecurity projects from different angles (of research and innovation but also deployment). In table 1 below, the main programs for digital sector in the new MFF have been presented, with a budget as presented by the European Commission in 2018 and expressed in current prices (2020).

Table 1. Main programs for the digital sector in the new MFF

Name of the program	Proposed budget in 2018	Final budget (in current prices)	Additional information
Digital Europe Program (DEP)	€8.2 bln	€9.2 bln	
Connecting Europe Facility (CEF Digital)	€1.8 bln	€2 bln	To support and catalyze investments in digital connectivity infrastructures of common interest
Horizon Europe	€94.4 bln	€105.8 bln	For research and innovation that will continue the work of Horizon 2020. Horizon Europe will be reinforced to fund vital research in health, resilience, and the green and digital transitions.
Invest EU	€31.6 bln	€34.4 bln	
Creative Europe Media	€1.5 bln	€1.7 bln	
EU4Health	€9.4 bln	€10.4 bln	With approximately 10% for digital transformation.

Name of the program	Proposed budget in 2018	Final budget (in current prices)	Additional information
Recovery and Resilience Facility (RRF)		€560 bln	According to the European Council Conclusions from 1 and 2 October 2020[5], each recovery and resilience plan should include a minimum level of 20% of expenditure related to the digital sector.

Source: own sources.

3. Cybersecurity in the new MFF - main programs dedicated to cybersecurity projects

3.1. Cybersecurity projects in Horizon Europe

Horizon Europe features a dedicated budget for six different clusters, including 'Civil security for society' and 'digital and industry'. The cluster called 'Civil security for society' consists of the following three areas: Cybersecurity, Disaster-resilient societies, and Protection and Security. Research and innovation in cybersecurity will support the use of innovative digital technologies, including self-healing, artificial intelligence, cryptography, massively distributed computing and storage, as well as quantum to increase data security and augment cybersecurity. It will further allow for security-relevant innovations in the areas of governance of algorithms, coding architecture, and programming languages. R&I will need to support the effectiveness and coordination of measures to respond to cyberattacks. It was agreed that research is necessary to better understand the nature and source of such attacks, as well as the technologies and strategies needed to counteract them. For all activities directed against cyberthreats, the architectural principles of 'security-by-design' and 'privacy-by-design' will be implemented in digital technologies and their applications, such as 5G, industry 4.0, artificial intelligence, Internet of Things, blockchain, quantum key distribution, mobile devices and connected cooperative and autonomous mobility and energy.

Regarding the 'Digital and industry' cluster, its goal is to develop research and high-end innovation in enabling technologies (artificial intelligence and robotics, next generation Internet, high performance computing and big data, key digital technologies, combining digital with other technologies). Taking into account the fact that the digital sector and green transition are the two main political priorities for the new European Commission and that they are

[5] https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf (access: 15.2.2021).