MASARYK UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY

VOLUME **16** | NUMBER **1** | SUMMER **2022** | ISSN **1802-5943**

PEER REVIEWED

CONTENTS:

www.mujlt.law.muni.cz

Masaryk University Journal of Law and Technology
issued by Institute of Law and Technology
Faculty of Law, Masaryk University
www.mujlt.law.muni.cz

Official Partner (Czech Republic)
ROWAN LEGAL, advokátní kancelář s.r.o. (www.rowanlegal.com/cz/)
Na Pankráci 127, 14000 Praha 4

Subscriptions, Enquiries, Permissions
Institute of Law and Technology, Faculty of Law, MU (cyber.law.muni.cz)

listed in HeinOnline (www.heinonline.org)
listed in Scopus (www.scopus.com)
reg. no. MK ČR E 17653

MASARYK UNIVERSITY JOURNAL OF
LAW AND TECHNOLOGY

VOLUME **16** | NUMBER **1** | SUMMER **2022**

LIST OF ARTICLES

DOI 10.5817/MUJLT2022-1-1

INSURANCE OF CYBER RISKS IN INTERNATIONAL TRANSPORT

by

PETR DOBIÁŠ*

The international transport of goods, passengers and luggage is recently facing the threat of cyberattacks. The article is focused on the analysis of the possible cyber risks in the field of the international transport and their management created by the international governmental and non-governmental organisations. The international regulation of the cybersecurity has only recommendatory character and will be subject to future development. That's the reason why should carriers pay greater attention to all possible cyber security measures. As the instrument of the reduction and mitigation of cyber risks could be used cyber-insurance. The insurance companies are offering insurance cover mainly on individual base corresponding to the extent of protection required by the policyholder.

KEY WORDS

Contractual Conditions, Cybersecurity, Insurance, Insurer, International Transport, Mitigation, Risk

1. INTRODUCTION

The technological progress in the field of management and operation of international transport of passengers and goods goes hand in hand with the implementation of the new advanced computer systems. The analysis provided in this article will be focused on the high technologies designed for the maintenance and operation of traffic systems used in the transport of goods, persons and their luggage. The significance of the analysis is underlined by the recent development in the field of maritime transport.

* E-mail: petr.dobias@vsci.cz, Assistant professor, CEVRO Institut, Chair of Private Law, Prague, Czech Republic.

The Maersk automated terminals were under cyber attacks[1] conducted by anonymous hackers in 2017,[2] which caused malfunction of the loading platforms at the port of discharge and led necessarily to the manual operation of the loading devices. Not only the landing ports, but also sea going vessels are not adequately protected against cyber-attack, because their operating systems are often old fashioned: the navigation software is subject the updates usually only during the necessary maintenance works or within the modernisation of the on-board navigation systems.

The navigation systems of the ships are on one hand well designed for the accident prevention, but on the other hand are also vulnerable to the security violation, because of the missing firewalls and other security features. The dual control systems and back up files are components of the most up-to-date operating systems only, which are present on the board of the sophisticated container vessels and ocean liners.

The malfunction of the GPS navigation systems and data corruption of the Electronic Chart Display and Information Systems (ECDIS) are usually excluded from the insurance cover. The target of a cyber attack could be also the largest maritime cargo vessel, the HMM Algericas, which can carry up to 23,964 containers (TEUs) at a time and cost over USD 140 million[3]. The vulnerability of the navigation systems could theoretically lead to the remote control of twelve naval vessels of this class in the property of HHM (formerly known as Hyundai Merchant Marine), each weighing 215,000 tonnes and measuring 399,9 meters in length.

It should be mentioned, that operators providing intelligent public transport services don't spend sufficient financial sources on development,[4] security and maintenance of security systems.[5] For that reason are state departments and agencies adopting measures for mitigation, planning and

---

1 Cyber attack is defined as "*attack on IT infrastructure in order to cause damage, or to obtain sensitive or strategically important information*" (Jirásek, P., Novák, L., Požár, J. (2015) *Výkladový slovník Kybernetické bezpečnosti*, Prague: PA CR in Prague, Czech branch of AFCEA, p. 71).

2 Saul, J. (2017): *Global shipping feels fallout from Maersk cyber attack*. [online] Thomson Reuters. Available from: https://www.reuters.com/article/us-cyber-attack-maersk/global-shipping-feels-fallout-from-maersk-cyber-attack-idUSKBN19K2LE/ [Accessed 1 January 2021].

3 Author not specified. *Say hello to HMM Algericas, the largest container vessel on earth* , [online] Shipping and Freight Resource. Available from: https://www.shippingandfreightresource.com/hmm-algericas-largest-container-vessel-on earth [Accessed 15 October 2021].

4 Innovative approaches to ITS security (blockchain, anonymous authentication in fog, bloom filter, security by contract and sensor fusion) are specified e.g. in Mecheva, T., Kanakov, N. (2020) Cybersecurity in Intelligent Transportation Systems, *Computers*, 9, 83, p. 6-8 [online]. Available from: www.mdpi.com/journal/computers [Accessed 10 November 2021].

monitoring, which are based on the recommendations of the penetration testers.[6] The main issue is the ignorance of the essential principles of cybersecurity in connection with the wrong understanding of the protection against cyber attacks in the area of the intelligent public transport service, which can be demonstrated on the outcomes of the European Union Network and Information Security Agency (ENISA) study on Cybersecurity and Resilience of Intelligent Public Transport. The study outcomes results in surprising finding, that 40 % of respondents confirmed hypothesis, that company at which they work does not test the functionality of the measures in the cybersecurity area.[7]

As the primary research question, which will be examined in this article, is to identify the risks associated with cyber attacks in international transport. A secondary research question will be to determine whether and to what extent the consequences of cyber attacks in international transport can be reduced using insurance.[8]

The research in this article will be based on research of the literature, when an analysis of the sources of the legislation, professional literature and Internet resources will be provided. The sources of information used will be subjected to critical evaluation and, based on a synthesis of the acquired knowledge, the author's own opinions will be expressed.

The primary research question will be solved in the theoretical part of this article on the basis of definition and analysis of cyber risks threatening in different modes of transport (case study approach). The secondary research question will be answered with the use of the comparative analysis. The author will look for answer to question, if the recent state of the cyber security risk in international transport could be reduced by the cyber risk insurance. As part of the assessment of the possibility of mitigating the risks associated with cyber attacks

[5] The security challenges in this area are in more detail analysed in Harvey, J., Kumar, S. (2020) A Survey of Intelligent Transportation Systems Security: Challenges and Solutions, Conference paper, May 2020, [online]. Available from: https://www.researchgate.net/publication/342405096 [Accessed 10 November 2021].

[6] Cf. U. S. Department of Transportation. (2019) Cybersecurity and Intelligent Transportation System, Best Practice Guide – September 17, 2019, Publication Number: FHWA-JPO-19-763, p. 35 [online]. Available from: www.its.dot.gov/index.htm [Accessed 10 November 2021].

[7] Lévy-Bencheton, C., Darra, E. (2015) *Cybersecurity and Resilience of Intelligent Public Transport, Good practices and recommendations*, Athens: ENISA, pp. 31 and 32.

[8] According to the recent survey 2,78% cyber insurance claims between 2013 and 2019 were located in transportation. (Source: Statista (2021) *Distribution of the number of cyber insurance claims made worldwide between 2013 and 2019, by industry*. New York: Statista Inc. Available from: www.statista.com/statistics/1190969/cyber-insurance-number-claims-industry-global [Accessed 25 June 2021]).

a comparison of insurance coverage offered in the insurance conditions of selected insurance companies will be conducted. To address the aim of this research, in the practical part of this article will be conducted analysis of insurance coverage, risk and premium based on the insurance terms and conditions.

2. THEORETICAL PART – DEFINITION OF CYBER RISKS IN INDIVIDUAL TYPES OF TRANSPORT

2.1 AIR TRANSPORT

2.1.1 INTRODUCTION TO CYBER RISKS IN AIR TRANSPORT

According to the press report published in 2015 was possible to successfully hack the guidance system of civil aeroplane due to lack of security software via universal series bus port mounted on the back of the passenger seat. The affected aeroplane control systems allowed the perpetrator experimentally change the trajectory of the flight. [9]

2.1.2 INTERNATIONAL REGULATION OF THE PROTECTION OF AIRCRAFT FROM CYBER ATTACKS

International governmental organisations are looking for solution based on the education and skill oriented training. The International Air Transport Association (IATA) clearly stated that increased reliance on data and connectivity will further exacerbate cyber security risks.[10] On that ground IATA created set of guidelines to mitigate cybersecurity risks[11]. It is a overview of international cyber security instruments, documents, standards and guidelines applicable to Civil Aviation Sector with recommendations and short commentaries. The cybersecurity in international air transport is also the strategic objective of the International Civil Aviation Organisation (ICAO). The ICAO introduced its Aviation Cybersecurity Strategy in October 2019.[12] The Aviation Cybersecurity strategy is based on seven pillars (1. International cooperation, 2. Governance, 3. Effective legislation and regulations, 4. Cybersecurity policy, 5. Information Sharing, 6. Incident

[9] Weise, E. (2015) Officials look into whether hacker really took over plane. *USA Today*, 17 May. Available from: https://eu.usatoday.com/story/tech/2015/05/17/hacker-sideways-chris-roberts-fbi-united/27492409/ [Accessed 21 June 2021].

[10] IATA, Airport Transport Security 2040 and Beyond, Version 1, 2019, p. 9.

[11] IATA. Compilation of Cybersecurity Regulations, Standards, and Guidance Applicable to Civil Aviation, Edition 2.0, April 2021.

[12] ICAO, Aviation Cybersecurity Strategy, Quebec, October 2019, p. 2-4.

management and emergency planning, 7. Capacity building, training and cybersecurity culture). ICAO also earlier issued working papers containing, in an annex, the Assembly's resolution on cybersecurity in civil aviation[13]. The problem is that the Action Plan on Cybersecurity in Civil Aviation only broadly declares a commitment to cooperation between the contracting states, which is specified in the Appendix A (Cybersecurity Action Plan Roadmap). ICAO should develop cybersecurity policy guidance to facilitate harmonisation and consistency amongst global, regional and national policies. National specific aspects ought to be justified and facilitate transnational compliance (Art. 7.3.1.). ICAO will conduct a review of the Action Plan on Cybersecurity in Civil Aviation as and when appropriate, but the Member States of ICAO cannot be sanctioned for noncompliance with the measures stipulated in the Action Plan. ICAO relies on content of arguments during intensive communication with the Member States,[14] allowing enforcement of measures scheduled in Appendix A. The priority should be given to work towards a common baseline for cybersecurity standards. According to the Art. 37 of the Convention on International Civil Aviation "*International Civil Aviation Organization shall adopt and amend from time to time, as may be necessary international standards and recommended practices*" dealing with i.e. communications systems and air navigation aids, rules of the air and traffic control practices, and such other matters concerned with the safety, regularity and efficiency of air navigation.

The Assembly's resolution on cybersecurity in civil aviation was adopted by the ICAO General Assembly at its meeting in the period from 27 September 2016 to 6 October 2016 in Montreal under No. A39-19. The Assembly's resolution on cybersecurity is also only of a recommendatory nature and, in addition, the activities set out therein were implemented by the 40th session of the ICAO General Assembly (Resolution A40-10: Addressing Cybersecurity in Civil Aviation), which took place from 24 September 2019 to 4 October 2019 and resulted in the approval of the ICAO Cybersecurity Strategy, which is again

[13] ICAO Working paper, Assembly – 39 Session, Executive Committee, Agenda Item 16: Aviation Security – Policy, Addressing Cybersecurity in Civil Aviation, A39-WP/17 EX/5, 30. 5. 2016, which was subsequently amended in the form of the ICAO Working paper, Assembly – 40 Session, Executive Committee, Agenda Item 12: Aviation Security – Policy, ICAO Cybersecurity strategy, A40-WP/28 EX/13, 25. 6. 2019.

[14] ICAO has 191 Member States recently.

of a recommendatory nature in relation to the Member States. In particular, ICAO calls on States Parties and civil aviation entrepreneurs to participate in the development of strategies to combat cyber crime, the establishment of governmental and non-governmental bodies to share information and minimise cyber risks, and the drafting of international and national legislation to protect against cyber risks in international aviation transportation.

The Study Group on Cyber Security in Civil Aviation (CYBER) is trying since 2013 to raise the level of awareness of cyber risks in European Civil Aviation Conference (ECAC) Member states.[15] On that ground the Study group is analysing recent developments of cyber-security control measures and giving guidance how to reduce risk of cyber-security attacks aimed on the critical aviation information systems.

2.2 MARITIME AND RIVER TRANSPORT

2.2.1 INTRODUCTION TO MARITIME CARGO TRANSPORT

In 2019, 7,907,300,000 tonnes of dry goods, 1,860,200,000 tonnes of crude oil, and 1,308,400,000 tonnes of refined petroleum products, gas and chemicals was transported by sea[16]. It is therefore surprising how inadequate the security measures on board cargo ships and in ports are. The state bodies[17] and bodies of governmental and non-governmental international organisations are implementing measures in order to the cyber risks[18].

2.2.2 ELECTRONIC SYSTEMS USED FOR THE CONTROL, COMMUNICATION AND NAVIGATION OF MARITIME AND RIVER VESSELS

System for displaying electronic navigational charts and information

The Electronic Chart and Display Information System[19] (ECDIS) is an electronic assistance system employed in the management of vessel. The cybersecurity of the ECDIS system is often underestimated by the ship--owners, who are implementing software and hardware components

[15] ECAC Doc. 30, chapter 14.

[16] Source: Barki, D. and Deleze-Black, L. (ed.) (2020) Developments in International Seaborn Trade. *UNCTAD Review of Maritime Transport 2020*, p. 7.

[17] E.g. in the United States of America this refers to the U. S. Department of Homeland Security.

[18] An example may be the IMO Guidelines on Maritime Cyber Risk management (IMO's Maritime Safety Committee, MSC-FAL.1/Circular 3, 5. 7. 2017), or the BIMCO Guidelines on Cybersecurity Onboard Ships (version 4, 2020).

[19] Note: The ČSN EN 61174 ed. 3 (367827) standard uses the translation System of Electronic Chart and Information Display.

of the navigational devices.[20] The ECDIS software is representing a security risk to ship navigation technology systems, which can be easy target for the cyber attack, because this software is simply integrated to the operational system of the on-board computer. ECDIS constitutes critical operational technology (software) designed for planning of the maritime voyage.[21] Crew management and members need to get basic safety training in order to prevent breach of discipline during the long voyages. Some crew members of maritime ships use USB ports connected to the ECDIS to play on-line computer games and to communicate with their families via smart phones, which may lead to interruption or collapse of the whole navigational system as a result of such activity[22].

Automatic identification system

In the maritime sector is used since 2002 as the supplement of the navigation systems the Automatic Identification System (AIS) which allows real-time location tracking of the vessels. The system provides important information related to the position of the ships for shore-based broadcasting stations and coastal authorities which is crucial for safe operation and anchoring of ships in their vicinity. The vessels equipped with AIS have possibility to locate the position of the ships within the distance of 20 nautical miles, even if they cannot be seen by the radar. The advantage and disadvantage of the AIS is, that the information's about the ship (course, position registration number etc.) could be found easily via many internet webpages, which are accessible without password and free of charge. The security risk rests in the AIS messaging system, which is unencrypted. It means, that messages including sensitive information, can be obtained by the hijackers (or pirates) with relatively cheap high frequency receiver.[23]

Global navigation system

---

[20] Svilicic, B., Brčić, D., Žuškin, S, Kalebić, D. (2019) Raising Awareness on Cyber Security of ECDIS, *TransNav*, 13 (1), p. 231.

[21] DiRenzo, J. et al. (2015) The *Little-known Challenge of Maritime Cybersecurity*. [online], p. 2. Available from: http://archive.dimacs.rutgers.edu/People/Staff/froberts/MaritimeCyber CorfuPaper.final.pdf [Accessed 4 January 2021].

[22] *The Nautical Institute*. Charging your phone on the bridge? Think again!, The Navigator, June 2016, pp. 6-8.

[23] Kessler, G. C., Craiger, J. P., Haas, J. C. (2018) Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System, *TransNav*, 12 (3), p. 432.

The Global Positioning System (GPS) is used as part of the AIS, that is why both systems can be affected by the same cyberattack. The dangerous hacker activities are focused merely on spoofing of the GPS system, because the jamming of this system leads to activation of the automatic alert system within the vessel's GPS module. The spoofing of the GPS may result in a fatal accident, which can be demonstrated on the maritime incident reported in the Black Sea in 2017.[24] For a few days GPS navigation devices gave an inaccurate inland position near Gelendyhik airport instead of correct position 25 nautical miles far away from it. In this context, should be mentioned experiment within the University of Texas project[25], as part of which a deliberately fraudulent signal was sent to a luxury yacht called "White Rose of Drax", whose automatic control system changed the course of the vessel in the wrong direction upon receipt[26]. For the disruption of the GPS signal is no need of very advanced capabilities, because the signal is usually very weak.[27] Hackers may also completely block the reception of signals by ships with outdated hardware and software.[28]

2.2.3 INTERNATIONAL REGULATION OF THE PROTECTION OF MARITIME VESSELS FROM CYBER ATTACKS

The International Ship and Port Facility Security Code was adopted on 12 December 2002 during the Conference of Contracting Governments to the International Convention for the Safety of Life at Sea (1974). The main objective of the code is to establish an international framework for detection and assessment of security threats including preventive measures against security incidents affecting ships or port facilities. International Maritime Organization (IMO) amended the International Ship and Port Facility Security Code[29] and the International Safety Management Code[30] in reaction

[24] Goward, D. (2017) Mass GPS Spoofing Attack in Black Sea? [online]. Available from: www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea [Accessed 26 November 2021].

[25] Press release on the project was published on 29. 7. 2013 at: www.news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/ [Accessed 4 January 2021].

[26] Muccin, E. (2015) *Combatting Maritime Cybersecurity Threats*. [online]. Available from: http://magazines.marinelink.com/Magazines/MaritimeReporter [Accessed 4 January 2021].

[27] Hambling, D. (2017) Ships fooled GPS spoofing attack suggests Russian cyberweapon *New Scientist* [online]. Available from: www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/ [Accessed 4 November 2021].

[28] Dobiáš, P. (2019) Kybernetická bezpečnost v mezinárodní přepravě se stále podceňuje, *Logistika*, 25 (1), p. 27.

[29] Revised version of 2017.

[30] International Safety Management Code, edition 2018, ID117E.

to increased incidence of cyberattacks. Here should be mentioned three fundamental problems specified by V. L. Forbes, which are related to the security of maritime vessels against cyberattacks. These include the obsolescence of maritime vessels' operating systems, the lack of training for vessel operating staff pertaining to management and protection against cyber attacks, and the lack of security for land-based communication facilities for maritime vessels[31]. Rolls Royce intends to gradually put into operation from 2021 remotely controlled autonomous vessels onwards, in order to reduce risk of a loss caused by the human element to a minimum. Information on the security of these vessels against cyber attacks is logically not known with regard to the company safety policy.[32]

2.3 ROAD TRANSPORT

2.3.1 INTRODUCTION TO CYBER RISKS IN ROAD TRANSPORT

The modern autonomous vehicles use specific deep reinforcement learning techniques for better recognition and avoidance of collision with obstacles, which could be remotely controlled by the perpetrator.[33] Recently were reported new security flaws in versions of Ford Focus and Volkswagen Polo, which can lead to data loss and malfunction of the electronic car management system. As the most vulnerable part of the car was proven the infotainment vehicle's system, which allows direct access to the personal data of the car owner and disabling of the automatic traction system.[34] This case demonstrates that drivers and passengers can be endangered by an attack on the system used to provide traffic and entertainment information to the driver and service information to the vehicle manufacturer.

An attack on a truck or a bus can also pose a really serious risk, given that efforts are being made to autonomously drive and automatically park

---

[31] Forbes, V., L. (2018) The *Global Maritime Industry Remains Unprepared for Future Cybersecurity Challenges*. [online] Available from: www.futuredirections.org.au/publication/the-global-maritime-industry-remains-unprepared-for-future-cybersecurity-challenges/ [Accessed 4 January 2021).

[32] Walker, J. (2018) *Autonomous Ships Timeline – Comparing Rolls-Royce, Kongsberg, Yara and More*. [online]. Available from: www.techemergence.com/autonomous-ships-timeline [Accessed 4 January 2021].

[33] Hahn, D., A., Munir, A., Behzadan, V. (2021) Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges, *IEEE Intell. Transp. Syst. Mag.*, 13 (1), p. 7.

[34] Which. (2021) Popular connected cars from Ford and Volkswagen could put your security privacy and safety at risk, Which? Finds, Which [online]. Available from: https://press.which.co.uk/whichpressreleases/popular-connected-cars-from-ford-and-volkswagen-could-put-your-security-privacy-and-safety-at-risk-which-finds/ [Accessed 26 November 2021].

even these vehicles. To this end, Jeremy Daily[35] recommends the use of a special test environment designed to improve safety standards and identify vulnerabilities in truck electronic control systems.

In road transport, a truck can also be monitored by camera systems located on motorway routes and other major urban and extra-urban roads. Toll and transit systems now automatically recognise and store vehicle registration plates. With the help of these systems, an attacker can not only determine the location of a vehicle, but also its speed, because many road camera systems are connected to devices for measuring the maximum permitted speed. This allows criminals to monitor a vehicle and more easily plan the act of physically breaking into a vehicle or a suitable moment to attack its control systems. Given that, in accordance with Article 7 of Regulation No. 561/2006[36], a truck driver must take a safety break after 4.5 hours of driving, perpetrators of criminal activity can calculate the time and place of that break relatively accurately. In addition, they can monitor the vehicle repeatedly and see if the driver leaves the vehicle in an unsecured place at night during transit. If the human driver is replaced by fully autonomous trucks, there is a danger not only of the possibility of remote control of the vehicle control unit[37], but also of the possibility of physically placing the perpetrator's device on the vehicle, if the perpetrator switches on the red light of traffic lights that the autonomous vehicle will pass through. A countermeasure may be to place a sufficient number of cameras and sensors on the truck. However, if the perpetrator manages to penetrate the vehicle's control system, he will usually control or paralyse these systems as well.

2.3.2 INTERNATIONAL REGULATION OF THE PROTECTION OF ROAD TRANSPORT FROM CYBER ATTACKS

On 22 January 2021 entered into force three UN vehicle regulations adopted by the World Forum for Harmonization of Vehicle Regulations created

[35] Daily, J. et al. (2016) Towards a Cyber Assurance Testbed for Heavy Vehicle Electronic Controls. *SAE International Journal of Commercial Vehicles*, 9 (2), p. 58.

[36] Regulation (EC) No. 561/2006 of the European Parliament and of the Council of 15 March 2006 on the harmonisation of certain social legislation relating to road transport and amending Council Regulations (EEC) No. 3821/98 and (EC) No 2135/98 and repealing Council Regulation (EEC) No 3820/85 *Official Journal of the European Union* (2006/L-102/1).

[37] The fact that even a sophisticated autonomous control system can be deceived was demonstrated in the past on a Tesla vehicle (Greenberg, A. (2016) *Hackers Fool Tesla S'S Autopilot to Hide and Spoof Obstacles* [online] New York: Wired. Available from: www.wired.com/2016/08/hackers-fool-tesla-ss-autopilot-hide-spoof-obstacles [Accessed 4 January 2021].).

within the framework of United Nations Economic Commission for Europe (UN Regulation No. 155 concerning the approval of vehicles with regards to cyber security and cybersecurity management system, UN Regulation No. 156 Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system and UN Regulation No. 157 on the type approval of automated lane keeping systems). This important legislative activity, which is based on the system of minimum requirements laid out especially in the above mentioned regulations No. 155 and 156, is limited to the Member states of UNECE only. But there it is assumed,[38] that regulators in Non-member states will be influenced by the UNECE standard.

The Regulation No. 156 covers all crucial aspects of cybersecurity across the entire motor vehicle lifecycle (management of cyber risks, ensuring security of vehicles by design, detection and response to security incidents and ensuring of safe software updates).

2.4 RAIL TRANSPORT

2.4.1 INTRODUCTION TO CYBER RISKS IN RAIL TRANSPORT

The Annex (Chapter V. Section B.) to the Regulation No. 432/2010 Coll., on the Criteria for Determining Critical Infrastructure Elements classify the Railway infrastructure as the element of critical transport infrastructure[39] (the critical infrastructure is defined in the Czech Republic in Act No. 240/2000 Coll., the Crisis Act, as the element of the critical infrastructure, or a system of critical infrastructure elements. The disruption

[38] Cf. Burkacky, O., Deichmann, J., Klein, B., Pototzky, K., Scherf, G. (2020) Cybersecurity in automotive: Mastering the challenge, report, McKinsey&Company, p. 7. Available from: www.mckinsey.com/industries/automotive-and-assembly/our-insights/cybersecurity-in-automotive-mastering-the-challenge# [Accessed 24 June 2021].

[39] According to the Annex II of the Directive (EU) of the European Parliament and of the Council of July 2016 concerning measures for high common level of security of network and information systems across the Union (NIS Directive) railway undertakings and infrastructure managers are classified as operators of essential services within the meaning of Art. 4 (4), if they meet the criteria laid down in Art. 5 (2). The criteria for the identification of the operators of essential services shall be: an entity provides a service, which is essential for the maintenance of critical or/and economic activities; the provision of that service depends on network and information systems; and an incident would have significant disruptive effects on the provision of that service. The Member States shall adopt and publish by 9 may 2018, the laws, regulations and administrative provisions necessary to comply with NIS Directive. E.g. in Germany is recognised railway infrastructure also as very important part of critical infrastructure (Regulation of 22 April 2016 for determination of Critical Infrastructure according to the BSI-Act. Federal Ministry of the Interior, Building and Community and Federal Ministry for Economic Affairs and Energy. In German.). This Regulation contains specific parameters for evaluation of the railway sites as the elements of critical infrastructure based on the number of passengers or weight of transported goods.

of the critical infrastructure could have a serious impact on the security of state, the provision of the basic living needs of the population, human health or state economy. This part of critical infrastructure needs special protection against cyber attacks, because of its vulnerability.[40] Today the technical state and position of the train is controlled by the track and rail monitoring systems and suitable measures can be initiated even before rail operations are negatively impacted. Functions such as real-time monitoring and tracking of railway vehicles can improve the overall rail system reliability,[41] but the railway management and control systems can be also hacked by criminals, who are motivated by a bid to obtain funds,[42] The cyberwarfare driven by political motivations could be found also in the railway sector.[43] We can speak about increasing threat of the terroristic attacks against high speed trains.[44]

2.4.2 INTERNATIONAL REGULATION OF THE PROTECTION OF RAILWAYS FROM CYBER ATTACKS

Within the COLPOFER[45] were created different working groups for the purpose of detection, prevention and elimination of security vulnerabilities in railway sector (e.g. cybercrime, terrorist and extremist activities). The main tasks of the working group established for prevention of cybercrime is to facilitate exchange of knowledge and information related to cybercrime in railway sector and to create recommendations regarding

---

[40] Fuchs, P. Rozová, D., Šustr, M., Šohajek, P. (2018) Critical Infrastructure in the Railway Transport System, Proceedings of the 22nd World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2018), p. 184.

[41] Ulianov, C., Hyde, P., Shaltout, R. E. (2018) Railway Applications for Monitoring and Tracking Systems. In: Marin Marinov (ed.) *Sustainable Rail Transport, Lecture Notes in Mobility*, Cham: Springer International Publishing, 2018, pp. 77-91.

[42] This conclusion could be demonstrated on recent cases in Czech Republic (David, J. (2021) Cyber Attack on Railways in the Czech Republic. Railtarget, 22 March [online] Available from: https://www.railtarget.eu/news/cyber-attack-on-railways-in-the-czech-republic-215. html [Accessed 24 June 2021]) and in United States of America (Goldbaum, Ch., Rashbaum, W. K. (2021) The M.T.A. Is Breached by Hackers as Cyberattacks Surge. New York Times, 2 June [online]. Available from: https://www.nytimes.com/2021/06/02/nyregion/mta-cyber-attack.html [Accessed 24 June 2021]).

[43] Clear example are Madrid train bombings (first attack was carried out on 11th March 2004). The second bombing on 2nd April 2004 directed against high-speed AVE train was not successful.

[44] In the United States was published already in 2006 study on Freight and Passenger Rail Critical Infrastructure Assessment warning over underfunding for security enhancements of all systems in American Public Transportation (Capra, G. S.: Protecting Critical Rail Infrastructure. The *Counterproliferation Papers*, Future Warfare Series No. 38, USAF Counterproliferation Center, p. 11), which exemplifies the initial underestimation of preventive measures in highly developed economy.

[45] This organisation operates in Europe and is one of the specialised groups within the International Union of Railways (UIC).

data protection. The European Union supported the Cybersecurity in the Railway Sector Project (CYRAIL), which was finished in 2018. During the international conference held in Paris (UIC Headquarters, 18 September 2018) were presented CYRail Recommendations on the cybersecurity of signalling and communication systems.[46] The main benefit to railway security is the CYRail Recommended system. The recommended security model is designed as alerting and collaborative 3-tier management system (1. detection system, 2. centralized alerting and monitoring system and 3. collaborative information sharing system).

2.5 PARTIAL CONCLUSION

Based on the analysis carried out during the preparation of this article, it was found that international transport faces insufficient training of staff operating means of transport[47] and the insufficient or even complete lack of security against cyber attacks. How else can it be explained that some vehicle crews use USB ports designed to update control system software to communicate on social networks[48] via their own devices?

There is still the idea, even among a large number of entrepreneurs, especially in maritime and air transport, that a means of transport far away from transmitters cannot be the target of a cyber attack. The cost incurred to protect against cyber attacks is low compared to the damage that a hacker attack can do. Obsolete means of transport can be easily exposed to cyber attacks if at least regular security software updates are not performed[49].

---

[46] CYRail Consortium Members. CYRail Recommendations on cybersecurity of rail signalling a communication systems. UIC-ETF, September 2018, ISBN 978-2-7461-2747-0.

[47] In the recent study on cyber security in transport by rail prepared within the EPSF (Établissement public de secúrité ferroviaire) was confirmed, that access required by maintenance staff must be brought under control (Établissement public de sécurité ferroviaire (2021) *Taking cybersecurity challenges into account in railway safety*. ENR135 – V1. Amiens: European Union Agency for Railways (ERA), French National Cybersecurity Agency (ANSSI), French National Safety Agency for Railways (EPSF), and SNCF Voyageurs and SNCF Réseau, p. 16).

[48] *The Nautical Institute*. Charging your phone on the bridge? Think again!, The Navigator, June 2016, pp. 6-8. Press release on the project was published on 29. 7. 2013 at: www.news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/ [Accessed 4 January 2021].

[49] For the sake of completeness, it is necessary to state that some transport companies cannot update the operating system without testing a new update of the operating system, because otherwise the operating system may crash (On this issue, compare Šulc, V. (2018) *Kybernetická bezpečnost*. Pilsen: Aleš Čeněk, pp. 95 and 96). This does not change the fact that most of the vulnerabilities that are subject to a cyber attack have been known for a long time at the time of the attack and are therefore not so-called day zero vulnerabilities.

Nor is it gratifying to note that sufficient importance is not placed on protection against cyber attacks at the international level, because significant expenses required for sufficient protection against cyberattacks, will raise the transport costs. In view of the costs required for hardware and software security, documents of a recommendatory nature are being developed within working groups and left to national legislation[50] as to how to regulate protection against cyber risks. Despite the European Union's efforts to regulate this area by secondary law and by supporting projects aimed at cybersecurity, the state of protection against cyber attacks is still insufficient.

3. PRACTICAL PART – MITIGATION AND ELIMINATION OF RISKS IN INTERNATIONAL TRANSPORT THROUGH INSURANCE

3.1. DEFINITION OF CYBER RISKS IN INTERNATIONAL TRANSPORT

In international civil transport may be subject to a cyber attack telematics – especially audio and visual equipment (traffic lights, audio warning equipment, traffic signals with variable display, etc.) and some other traffic equipment (barriers, inlet closures, locks, automatic sliding bollards, lifting bridges, etc.). Usual subject of a cyber attack are also means of transport in road, air, rail, maritime and inland waterway transport. Within the maintenance and operation of vehicles is required protection of service stations and filling stations for the pumping of fossil fuels or the charging of electric vehicles. Specific measures shall be adopted for protection of public transport stations and computer systems used to record passengers, baggage and goods. The necessity for strict measures could be demonstrated on Air India,[51] Brittish Airways[52] and Lufthansa[53] personal data leaks. The attention shall be paid to protection of infrastructure

[50] According to § 2(i) of Act No. 181/2014 Coll., on cybersecurity, a basic service is a service the provision of which depends on electronic communication networks or information systems, and whose disruption could have a significant impact on the security of social and economic activities, e.g. in the transport sector.

[51] Page, C. (2021) Air India Data Breach: Hackers Access Personal Details Of 4.5 Million Customers. *Forbes*, 23 May. Available from: https://www.forbes.com/sites/carlypage/2021/05/23/air-india-data-breach-hackers-access-personal-details-of-45-million-customers/ [Accessed 25 June 2021].

[52] MacGregor, L. (2019) British Airways faces largest ever data breach fine for 2018 hack. *New Scientist and Press Association.* 8 July. Available from: https://www.newscientist.com/article/2208964-british-airways-faces-largest-ever-data-breach-fine-for-2018-hack/ [Accessed 25 June 2021].

necessary for proper and safe functioning of all modes of transport (warehouses and transhipment points, including their equipment – e.g. cranes and trucks, traffic control centres – airport navigation towers, radars, sea beacons and stationary or portable navigation systems).

The cyber attacks can disable security devices used to detect the danger of fire, accidents of means of transport, etc., which are crucial for mitigation of damages and personal injury.

In the case of a cyber attack on the equipment listed in previous paragraph, the following consequences may occur, for example:

a) traffic accidents at an intersection or railway crossing due to non--functioning signalling and security,
b) control of the vehicle by the attacker and its destruction, damage or theft,
c) explosion of a filling station, leakage of dangerous substances, or refueling of fuel or energy by a perpetrator free of charge,
d) inoperative service mechanism preventing the repair of vehicles or causing damage to them,
e) theft of goods from a warehouse or control of their equipment and causing of damage,
f) stopping public transport of persons, or guiding means of transport into a collision course resulting in an accident, or controlling air conditioning or a fire extinguishing system,
g) causing a navigation system to malfunction, resulting in the need to switch to manual backup systems and controls with an increased risk of accidents,
h) transmission of a false GPS signal in order to change the course of the autopilot,
i) misuse of passenger information (personal data, data from a means of payment, etc.) for the purpose of the use of such data, sale or extortion,[54]

[53] DPA/AFP. (2015) Hackers break into Lufthansa customer database. *Deutsche Welle*,10 April. Available from https://www.dw.com/en/hackers-break-into-lufthansa-customer-database/a-18374698 [Accessed 25 June 2021].

[54] S. Wares and V. Thompson, are mentioning loss and deletion of data, which could be consequence of non-payment for unblocking of encrypted passengers database (Wares, S., Thompson, V. (2015) *Marsh Insights: Cyber Risk in the Transportation Industry*, p. 1 [online]. Available from: https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/Cyber%20Risk%20in%20the%20.Transportation%20Industry-03-2015.pdf [Accessed 4 January 2021]).

j) dysfunction of the security equipment enabling the prevention of collisions of vehicles or their fire.

Gina Tonn, Jay P. Kesan, Jeff Czajkowski and Linfeng Zhang[55] present the following general ways to prevent cyber damage:

a) development of methods that will improve the system architecture and activities,
b) operating methods involving changes in business transactions,
c) countermeasures, including the acquisition of security software, the design of the system, the improvement of the course of operations and investment in the cybersecurity workforce,
d) security measures including firewalls, encryption software, a virus detection system, and the division of the system into several parts.

As another possible breakdown of cyber risk management measures, they[56] state the division into:

a) institutional measures (software and hardware),
b) procedural measures (management systems and operating systems),
c) responsive measures (response and damage management after a security incident has been detected).

The above authors come to the unequivocal conclusion that the growing number of cyber attacks and the damage they cause will lead to efforts to transfer risk to insurance companies through cybersecurity insurance, especially for entrepreneurs[57,58]. What cannot be fully agreed with is the claim of these authors that a risk is arising that policyholders will not take sufficient measures in the field of cybersecurity, as they will rely on insurance companies to compensate for the damage they cause.[59] Given that insurance companies are likely to want part of the insurance portfolio

[55] Tonn, G., Kesan, J. P., Czajkowski, J. and Zhang, L. (2018) *Cyber Risk and Insurance for Transportation Infrastructure*, p. 3 [online]. Available from: https://riskcenter.wharton.upenn.edu/wp-content/uploads/2018/03/WP201802_Cyber-Security-Transportation-Sector.pdf [Accessed 4 January 2021].

[56] Ibid, p. 4.

[57] Ibid, p. 3.

[58] We can find contrary opinion in the study of K. Quigley and J. Roy, who are disputing possibility to use insurance for the transfer of risk to insurance company, because „the failures are too difficult to model, and therefore impossible to cost" (Quingley, K., Roy, J. (2011) Cyber-Security and Risk Management in an Interoperable World An Examination of Governmental Action in North America, *Social Science Computer Review*. 30 (1), p. 86. Available from: http://ssc.sagepub.com/content/30/1/83 [Accessed 24 June 2021]).

[59] Transfer of risk is recognised as one of five main risks control strategies (Cf. Kure, H. I., Islam, S., Razzaque, M. A. (2018) An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. *Applied Sciences*, 8 (6), p. 16. Available from: www.mdpi.com/2076-3417/8/6/898 [Accessed 25 June 2021]).

comprised by insured cyber risks to be covered by reinsurance, it can be expected that, given the principle of capital adequacy, reinsurance undertakings will not be willing to take out insurance against insurance of risks for which it is difficult to determine at least the approximate scope of the damage. Insurance companies will therefore require, particularly for insurance of large insurance risks within the EU, that insurers take measures to reduce the probability of the occurrence of an insured event. Large insurance risks are defined in the Solvency II Directive[60] as a group of risks which are typically arising out of entrepreneurial activities. According to Article 13 (27) of the Solvency II Directive, large insurance risks include, inter alia, insurance of railway rolling stock, aircraft and vessels, including the goods transported and liability for the use of such means of transport[61]. However, it is difficult to determine the extent of damage incurred in transport during previous years. Although data on the number of cyber incidents is available on the Internet[62], only few statistics specify the resulting damage.[63,64] The uncertainty posed by the abovementioned issues arising out during the process of assessing the insurance risk leads to the situation, that there are few entities that specialise in cyber risk insurance in international transport[65]. In addition, many carriers rely on the fact that unless cyber risk insurance is excluded

[60] Directive (EC) 2009/138 of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) *Official Journal of the European Union* (2009/L-335/01).

[61] Insurance of ground vehicles (besides the railway fleet) is one of the major insurance risks only if the policyholder exceeds the limits for at least two of the criteria set out in Article 13(27) of the Solvency II directive.

[62] According List of data breaches and cyber attacks of 2020 there were reported 15 data breaches in transport and automotive (Irwin, L. (2021) 2020 cyber security statistics, IT Governance Available from: www.itgovernance.co.uk/blog/2020-cyber-security-statistics [Accessed 24 June 2021]).

[63] According to the summarized Assessment report of AIG designed for the client with annual revenue 51.000.000 USD the Data Breach Impact (median impact value per record volume) will be in case of low impact breach 85,712,026 USD for company with 100 millions records (AIG. (2020) *Cyber Insurance Summarized Assessment Report*, American International Group, Inc. Available from: www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyber-summarized-assessment-report-sample.pdf [Accessed 24 June 2021]).

[64] M. Bentley et al. hold an opinion that only limited data on cyber incidents are available and thus it is very difficult to get data pertaining to the losses suffered by one organization (Bentley, M., Stephenson, A., Toscas, P., Zhu, Z. (2020) A Multivariate Model to Quantify and Mitigate Cybersecurity Risk, *Risks*, 8 (61), p. 2. Available from https://doi.org/10.3390/risks8020061 [Accessed 24 June 2021]).

[65] An example of such a company is Marsh Ltd., an insurance intermediary based in London, which also deals with the assessment of insurance risks in international transport, or Jardine Lloyd Thompson Group plc, also based in London.

under an explicit exemption from insurance coverage, the insurance also covers these insurance risks.[66]

3.2. INSURANCE AGAINST CYBER RISKS IN INTERNATIONAL TRANSPORT

3.2.1. SYSTEMATIC INCLUSION OF CYBER RISK INSURANCE IN INTERNATIONAL TRANSPORT

Cyber risk insurance is non-life insurance[67] from the public law perspective and indemnity insurance from the private law perspective. According to Art. 1:201 (3) of the PEICL,[68] "indemnity insurance means insurance under which the insurer is obliged to indemnify against loss suffered on the occurrence of an insured event." The consequences of the insured event must be measurable in money. The purpose of indemnity insurance is therefore to compensate for loss resulting from an insured event[69]. Within the scope of indemnity insurance for cyber risks it is possible to arrange:

a) property insurance,

b) legal expenses insurance; and

c) liability insurance.

Property insurance will mainly cover means of transport and equipment. Legal expenses insurance will cover the elimination and minimisation of the consequences caused by a cyber attack, e.g. in the event of data leaks from a database of clients[70] and passengers, or in the case of legal representation costs in damages proceedings against a hacker. Liability

---

[66] In the study on silent cyber coverage in insurance provided by Leibnitz University Hannover - Institute for Risk and Insurance (Wrede, D., Stege, T., Graf von der Schulenburg, J.-M. (2020) Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market. The *Geneva papers on Risk and Insurance – Issues and Practice*, 45 (4), p. 657-689. Available from: www.repo.uni-hannover.de/handle/123456789/10772 [Accessed 24 June 2021]) was confirmed, that German insurers „have not yet developer holistic strategies for managing silent cyber exposures. Silent cyber exposures require systematic identification and quantification since the involved claims burdens are hard to estimate for insurers." This study supports the conclusion, that the cyber insurance is still unexplored branch of insurance designed for specialised insurers.

[67] The same is valid for the classification of risks according to classes of insurance in the framework of Directive Solvency II (Annex I).

[68] Basedow, J., Birds, J., Clarke, M. Cousy, H., Heiss, H. Loacker, L. (2016) *Principles of the European Insurance Contract Law*, 2nd ed., Cologne: Otto Schmidt, pp. 33 and 77.

[69] Karfíková, M. et al. (2018) *Insurance Law*. Prague: Leges, p. 307.

[70] An example is the case of the shipping company OutWest Express, whose computer servers were attacked by ransomware, which allowed hackers to gain access to data from a customer database and to order fictitious transport of goods in order to solicit cash advances from transport agents (Kilcarr, S. (2015) *Battling a hack: One fleet's story*. [online] Fort Atkinson: Fleetowner. Available from: https://www.fleetowner.com/technology/article/21692058/battling-a-hack-one-fleets-story [Accessed 4 January 2021]).

insurance will cover the obligation of the policyholder (carrier) to compensate for the damage arising to the damaged party to the extent and in the amount specified by law or contractual agreement.

3.2.2. CONDITIONS OF CYBER RISK INSURANCE

The insurance conditions of cyber risk insurance have a significantly more extensive structure and contain a more detailed regulation of the rights and obligations of the insurer and the policyholder in comparison with the insurance conditions of the insurance of internet risks concluded as part of household insurance. The content of the general insurance conditions is also a casuistic in its character.[71] The content of these conditions can be demonstrated on the insurance product called CYBERPLUS – CYBER RISK INSURANCE[72] and Cyber Enterprise Risk Management[73].

CYBERPLUS insurance forms the basic coverage, which can be variably extended with modules of optional extension coverage. The basic scope of insurance consists of claims for compensation for the damage caused by unauthorised handling of personal data and confidential information to the insured or his subcontractors, claims against the insured due to a breach of network security, costs of regulatory proceedings[74] and costs of professional services (cyber experts and independent consultants in the fields of law, media strategy, crisis management and personal relations).

Insurance coverage can be extended by the following areas:

a) publishing digital content in multimedia,

b) blackmail through a computer network,

c) network failure.

The insurance conditions of Cyber Enterprise Risk Management include the scope of insurance coverage, which in principle corresponds to CYBERPLUS insurance. It is therefore an insurance covering

---

[71] Romanosky et al. in their study focused on insurance policies from state insurance commissioners across New York, Pennsylvania, and California found that the covered losses appeared more consistent across all policies, whereas exclusions were more varied (Romanosky, S., Ablon, L., Kuehn, A., Jones, T. Content analysis of cyber insurance policies: how do carriers price cyber risk? *Journal of Cybersecurity*, 5 (1), p. 4. Available from: https://doi.org/10.1093/cybsec/tyz002 [Accessed 23 June 2021]).

[72] Insurance conditions of Colonnade, version CP 01-05/2019.

[73] Insurance conditions of Chubb European Group, version ERM 1-2016.

[74] According to Article 3.24, regulatory proceedings mean "*any proceedings against the Insured or an investigation or audit of the Insured conducted or carried out by the Supervisory Body (i) due to the use or alleged misuse of Personal Data; or (ii) for the purpose of verifying the procedures for the management and processing of Personal Data; or (iii) arranging such processing via a Subcontractor, to the extent regulated by the Personal Data Protection Guidelines*."

unauthorized handling of data, liability for breaches of network security, media liability, cyber blackmail, loss or corruption of data and interruption of operation.

According to Article 3.11, Cyber Enterprise Risk Management insurance also covers a cyberterrorism attack, while CYBERPLUS does not cover any losses resulting from or otherwise related to war and terrorism according to Article 4.11[75]. In the case of vehicle and equipment insurance, it will also be appropriate to arrange insurance against cyberterrorist attack, because the goal of cyberterrorists may be to take charge of the control systems of an aircraft, train or seagoing vessel in order to obtain a ransom. From the point of view of Czech criminal law, cyberterrorists may commit the crimes of sabotage, a terrorist attack, general endangerment, damage and endangerment of the operation of a public benefit facility or damage to another's property in the transport area[76]. Among the above-mentioned crimes, Václav Jirovský emphasises those that could endanger transport systems, or air traffic, the last of these offenses, as it involves attacks on telecommunications equipment[77]. This view can be accepted, as damage or manipulation to the navigation and communication systems of air traffic control can have fatal consequences, including aircraft crashes.

The limits of indemnity are not specified in the insurance conditions of CYBERPLUS or Cyber Enterprise Risk Management, which can be considered logical with regard to the fact that insurers will arrange this type of insurance according to the individual needs of the policyholder. When arranging special insurance for international transport, the degree of insurance risk is, as a rule, first assessed by means of distance communication. The following is an assessment of the extent of cyber risks related to the person interested in insurance and the determination of proposals for the scope of insurance coverage.

At the same time, the insurer or insurance intermediary simulates, with the person interested in the insurance, situations that may occur in the event of an attack on the means of transport and equipment of the person interested in the insurance. As soon as the person interested in the insurance chooses a suitable variant, a draft agreement containing

[75] As to the definition of the term cyber terrorism, compare Morán Blanco, M., S. (2017) La Ciberseguridad y el uso de las tecnologías de la información y la comunicación (TIC) por el terrorismo. *Revista Española de Derecho International*, 69 (2), p. 202.

[76] Smejkal, V. (2018) *Kybernetická kriminalita,* 2nd ed. Pilsen: Aleš Čeněk, p. 104 f.

[77] Jirovský, V. (2007) *Kybernetická kriminalita*. Prague: Grada, p. 95.

a detailed specification of the cyber risks covered by the insurance and exclusion from the insurance, is ready for this potential insured to sign.

3.3. INSURANCE RISK AND PREMIUM AMOUNT

It is difficult to ensure the complete cybersecurity in the case of international transport insurance. There is a need not only for effective software security but also to ensure physical security in the case of this type of insurance, more than in other cases. In the case of securing a means of transport, it will be necessary to effectively prevent the perpetrator from entering, in particular, the vehicle's control systems and the traffic management system. The problem is that a means of transport has to cover long distances and is parked in places with various levels of security during breaks. The question is how service depots for rail vehicles are secured, from which train carriages often leave marked with graffiti. What obstacle for a cyber criminal is posed by a service door locked with a square key and the entrance door to the driver's cab locked with an ordinary cylinder lock? Another example is airport security. Can an airport whose be considered as being sufficiently secure if amateur photographers had roamed on its apron in the past? What can be the consequences of being able to slide under or throw over a counter adjacent to the security checkpoint at an airport a replica of a military grenade? These security incidents will undoubtedly result in insurance companies requiring the performance of penetration tests and to assess, on the basis of these tests, the insurance risk and determine the amount of the premium individually. According the recently published opinion of M. Eling, M. McShane and T. Nguyen during the risk management process, interaction exists between risk mitigation and the purchase of insurance, that is, insurance purchasers typically pay lower premiums by investing more in risk mitigation.[78]

Jan Kolouch[79] presents a range of four basic measures relating to ensuring physical security:

a) securing the perimeter,

b) access control,

c) internal security,

d) protection of computer systems.

---

[78] Eling. M., McShane, M., Nguyen, T. (2021) Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, 24, p. 96. Available from: www.onlinelibrary.wiley.com/doi/epdf/10.1111/rmir.12169 [Accessed 25 June 2021].

[79] Kolouch, J., Bašta, P. et al. (2019) *Cybersecurity*. Prague: CZ.NIC, p. 411.

In the case of international transport, the problem is that the perimeter covers not only the whole airport or port but, as demonstrated above, in the past cyber attacks have succeeded in confusing the navigation system of a maritime vessel, and thus this is also probably possible for aircraft. Nevertheless, it will be primarily necessary to protect means of transport and equipment from cyber attack. The problem is how to protect traffic signals, boom gates and other similar equipment, which often operate in semi-automatic or fully automatic mode, from cyber attack. A similar situation arises in the case of lifting bridges and switches, which today are often controlled only remotely, with no human service staff found in their vicinity that could avert danger in the case of a physical attack to the equipment. It is true that this equipment tends to be monitored via camera systems or is connected to a central security desk, but the risk of deception of motion sensors or camera systems cannot be ruled out. The range of service and security units in the event of a cyber incident is also a problem. The subject of the attack may also be the means of transport themselves – it does not have to be exclusively a propulsion unit. It is also conceivable to deactivate an electronic measuring device on a freezer container or a gyroscopic device monitoring the movement of a container with an explosive and volatile substance. In the first case, only the transported food can be destroyed, while in the second case, there can be an explosion and damage to the life, health and property of people.

3.4. INSURANCE COVERAGE IN THE CZECH REPUBLIC AND THE UNITED KINGDOM

Insurers domiciled in the United Kingdom have wide experience with the cyber insurance. For this reason the insurers place emphasis on claim prevention of cyber incidents[80] and mitigation of damages caused by hacker. Efficient standard instrument offered by the insurance companies is 24/7 hours help desk for customers,[81] allowing policyholder to get immediate advice in case of imminent or ongoing attack. Customers

[80] J. Barlatier holds the view, that „*the prevention of cyber threats by private actors is based on risk anticipation and the immediacy of the threats.*" (Barlatier, J. (2020) Criminal Investigation and Criminal Intelligence: Example of Adaptation in the Prevention and Repression of Cybercrime. *Risks*, 8 (99), p. 8. Available from https://doi.org/10.3390/risks8030099 [Accessed 23 June 2021]) This approach to cyber insurance is evident with regard to many instructional material provided by British insurers free of charge via internet (booklets, manuals, guidelines, statistics etc.).

[81] In the Czech Republic is 24/7 customer support offered in the insurance of cyber risks by ČSOB Pojišťovna (General Insurance Conditions – Insurance of Cyber Risk, version VPP CRC 2018).

who are using help desk can also consult adviser for the purpose of adoption adequate precautionary measures. This access of insurers allows quick response to data or system breach, coverage of the costs associated with fines, ransom payments or notifications, which can be damaging to business of transport company, both in financial and reputational terms. The English insurers are trying by the way of preventive measures to reduce the risk of a loss to a minimum.[82] The insurers are publishing recommendatory publications, which are available free of charge on the internet not only to own customers but also potential customers and general public. The British insurers are providing customers with explanatory booklets in order to prevent misunderstanding and conflicts (e.g. in relation to software updates, firewall protection and virus protection).

Cyber insurance coverage is divided between first-party liability coverage (e. g. business interruption, cyber incident response, digital data recovery, network extortion, telephone toll fraud) and third-party liability coverage (e. g. cyber liability, media liability, network liability, privacy liability, regulatory proceedings).[83] Because of the competition between the insurers domiciled in the United Kingdom, the insurance cover tends to be all-encompassing including first party cover, third party cover, call centre costs, cyber terrorism, increased costs, employee data, reputational harm and transmission of computer virus.[84] The wide insurance cover is often subject to exemptions included in the insurance conditions which

[82] This recent trend was confirmed in report prepared for the Association of British Insurers (Oxera. (2020) The value of cyber insurance to the UK economy, Oxford: Oxera Consulting LLP, p. 12. Available from: www.oxera.com/insights/reports/the-value-of-cyber-insurance-to-the-uk-economy/ [Accessed 23 June 2021]).

[83] Cf. also theoretical concept of differences between first-party liability coverage and third-party liability coverage in Romanosky, S., Ablon, L., Kuehn, A., Jones, T. Content analysis of cyber insurance policies: how do carriers price cyber risk? *Journal of Cybersecurity*, 5 (1), p. 5. Available from: https://doi: 10.1093/cybsec/tyz002 [Accessed 23 June 2021]).

[84] Cf. AIG CyberEdge, version 010719 of 2019; Aviva Insurance Limited, Your insurance policy, version BCOAG 15628 (V36) 02.2021; HISCOX Cyberclear, Cyber and data insurance - policy wording, version WD-PIP-UK-CCLEAR(1) 19029 12/18; Markel UK Limited, Cyber and data risks, version CDR122016; NIG Cyber cover policy, version NIG101423/10/19.

shall be modified[85] according to the specific interest of the policy-holder (cyber policy is sometimes modular).[86]

To compare insurance coverage, we will choose the insurance conditions of Hiscox Limited for cyber and data protection[87]. Although this is an insurance company operating in the United Kingdom, the scope of insurance coverage is, as far as its basic elements is concerned, the same as for insurance companies domiciled in the Czech Republic. Insurance coverage includes interruption of connection, interruption of business activities, damage caused by hackers, cyber extortion, protection of personal data and liability in connection with the media. Similar insurance conditions (Cyber Risk Insurance Policy) are offered in the United Kingdom by Royal & Sun Alliance Insurance plc[88]. This is not a surprising finding, as AIG and Chubb European Group essentially operate worldwide and therefore know the insurance conditions of other insurance companies in the area of cyber risk insurance. The difference between the Czech Republic and some countries lies in the length of cybercrime experience, which can be manifested on clear terminology used in the insurance terms and conditions. Statistics in this area are already available abroad and procedures have been tested on how to proceed in the event of a cyber attack[89].

In the United Kingdom, tailor-made insurance for international transport is also offered. An example of such an insurance product is

---

[85] In a structured dialogue with insurance companies European Insurance and Occupational Pensions Authority (EIOPA) came to conclusion, that „vast majority of the insurers surveyed adopt a focused approach to cyber insurance and tailor products according to the client companies size and needs." (EIOPA. Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies. EIOPA, 2. 8. 2018. Available from: www.eiopa.europa.eu/content/understanding-cyber-insurance-structured-dialogue-insurance-companies_en [Accessed 4 June 2021]).

[86] For analysis of negotiations conducted in order to determine whether to underwrite a cyber risk cf. Nurse, J., R., C., Axon, L., Erola, A., Agrafiotis, I., Goldsmith, M., Creese, S. (2020) The Data that Drives Cyber Insurance: A Study into the Underwriting and Claims Processes, Conference Paper, p. 3. Available from: https://www.researchgate.net/publication/340849886_The_Data_that_Drives_Cyber_Insurance_A_Study_into_the_Underwriting_and_Claims_Processes/link/5f521074a6fdcc9879ca0a2d/download [Accessed 24 June 2021].

[87] HISCOX Cyberclear, Cyber and data insurance - policy wording, version WD-PIP-UK-CCLEAR(1) 19029 12/18.

[88] Cyber protection - policy wording, version UK 05239 A from19 September 2018.

[89] Cf. Egan, R. et al. (2019) Cyber operational risk scenarios for insurance companies. *British Actuarial Journal*, 24, e6, pp. 1-34. Available from: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/C90FF5F4EC6682A01E91F4E63A05F961/S1357321718000284a.pdf/cyber_operational_risk_scenarios_for_insurance_companies.pdf [Accessed 4 January 2021].

Shoreline Ltd's Integrated Cybercrime Insurance[90] for maritime transport[91]. This insurance covers costs incurred in connection with cyber theft, social engineering, interruption of business activities, investigation, extortion claims, liability for damage caused by third parties, mitigation of the consequences of a cyber attack and costs incurred without delay by the policyholder on minimising damage caused by data leakage, computer system malfunctions and breaches of third party privacy and security. It is interesting to note that the insurance cover applies to the interruption of business activities lasting at least eight hours. An example of such a situation, as provided in the scope of insurance, is the case where the vessel will not be able to be steered due to the interruption of access to electronic navigational charts. Another product that can be mentioned is CyNav insurance, intended to cover marine cyber risks, which also covers damage to vessels and machinery as a result of a cyber attack[92]. Given its size and geographical location of the UK, the insurance market in the United Kingdom is able to provide significantly more specific products in the field of cyber transport insurance than is the case in the Czech Republic.

British insurers have very precisely defined policy exemptions to prevent unfounded claims and related disputes. Some conditions are surprising and that's why policy-holder should read insurance terms precisely. Aviva insurance limited will not cover insured person for more than one claim arising out form the same cyber extortionist.[93] Markel will not pay a claim arising out of the data liability or cyber liability, where the claim is brought in a court of law outside the jurisdiction of the applicable courts shown in the policy schedule, and/or, where action for damages is brought in a court within that jurisdiction to enforce a foreign judgment.[94] Some insurers exclude in the United Kingdom from

[90] Integrated Crime Cyberinsurance for Marine Transport Industry. Available from: https://www.shoreline.bm/downloads/ICCI-Product-Info-Sheet.pdf?v=1585231040 [Accessed 4 January 2021].

[91] Shoreline Ltd is seated in Hamilton, Bermuda. Bermuda is one of United Kingdom's overseas territories, and is therefore included in this insurance coverage comparison. In addition, the insurer is Maritime Insurance Solutions, which is reinsured by Lloyd's.

[92] *CyNav*. (2020) Navigating shipowners' cybersecurity risks. Available from: https://www.willistowerswatson.com/en-GB/Solutions/products/cynav-navigating-your-cyber-security-risks [Accessed 4 January 2021].

[93] Aviva Insurance Limited, Your insurance policy, version BCOAG 15628 (V36) 02.2021, p. 5.

[94] Markel UK Limited, Cyber and data risks, version CDR122016, p. 4.

the insurance cover terrorism, but they offer supplementary insurance based on specific conditions.[95]

3.5. PARTIAL CONCLUSION

Based on the analysis carried out in the practical part, it was found that cyber risk insurance in international transport is a non-life loss insurance, and may include property insurance (e.g. damage related to network security breaches, network outages, hacker attacks, or cyber extortion), legal expenses insurance (legal representation in proceedings relating to damage or other harm caused by a cyber attack) and liability insurance (breach of privacy, confidential information and personal data; media liability). In the cyber risk insurance area, there exists a close connection with the regulation governing the protection of personal and sensitive data according to Act No. 110/2019 Coll., on the processing of personal data and on amending certain laws, and Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of the personal data of individuals with regard to the processing of personal data and on the free movement of such data and repealing of Regulation (EC) 95/46 (General Data Protection Regulation)[96], as cyber risk insurance also covers the unauthorised handling[97] of personal data by the insured and his subcontractors.

Based on a comparison of the content of the insurance conditions for Internet risk and cyber risk insurance, it was found that cyber risks insurance is usually taken out with entrepreneurs, and insurance companies have prepared separate conditions for this type of insurance. These contractual conditions for the property and liability insurance of entrepreneurs are modified for the purposes of international transport insurance.

The insurance of cyber risks offered by insurance companies in the Czech Republic is identical in their basic elements. The differences lie in the scope of insurance coverage. The limits of insurance indemnity are negotiated individually according to the needs of the policyholder or the insured. The scope of cyber risk insurance is similar in comparison

[95] NIG Cyber cover policy, version NIG101423/10/19, p. 9 and 25.

[96] Took effect on 25 May 2018.

[97] This may involve the unauthorised collection, management, storage, disposal or other processing of personal data. However, it must not be an intentional unauthorised collection of personal data or the intentional processing of personal data in violation of legal regulations.

with selected insurance conditions used by insurance companies operating in other countries.

4. CONCLUSIONS

The subject of the analysis carried out in the first part of the article was to define the risks that arise in connection with cyber attacks in the international transport of goods. The individual types of transport were interpreted, which were divided in terms of the means of transport used. In the theoretical part of this article, it was found that the subject of a cyber attack can be physical attacks on hardware as well as software. In the case of an attacker's physical intrusion into the perimeter within which means of transport and equipment are located, the attacker risks easier detection and detention, but in some cases these attacks allow for the easier and faster control or manipulation of the system under attack, to which the attacker's devices are permanently or temporarily connected. In this area, it is clearly evident that a great risk is posed not only by the lack of computer equipment security, but also the negligence or intentional actions of their operators. Another element of vulnerability that was identified is the possibility of transmitting a false signal, which allows you to manipulate the positioning and associated navigation equipment. Legislative measures in this area are not yet sufficient, which is the reason why international governmental and non-governmental organisations are seeking additional regulation. However, the documents of such legislative measures are usually legally non-binding, i.e. recommendatory in nature.

Legislation as well as resources drafted and made available by international organisations usually respond retrospectively to cyber risks that have already arisen.

The aim of the second part of the article was to answer the question of whether it is possible to reduce or eliminate the risks associated with cyber attacks by taking out insurance. In this case, the purpose of insurance is to transfer the risks associated with cyber attacks to the insurance company, which arises if the legal and insurance conditions are duly met. The most insurance contracts in this area are tailor-made for the policyholder. Transport companies are already under-insuring the goods they transported, because comprehensive insurance, which would pertain to the entire period of transport and cover the full value of the goods, is very expensive. Therefore, it will always depend

on the specific case as to what limits of insurance benefits and exclusions from insurance will be agreed upon. In the case of insuring other transport equipment against cyber attacks, it will sometimes be difficult to determine the optimal limits of indemnity and to set the corresponding amount of indemnity. The starting point for negotiating suitable insurance conditions may be accounting or an estimation of the amount of damage arising based on model cyber attacks. The final form of the insurance contract and the insurance conditions will therefore always be a compromise between the requirement for an adequate amount of indemnity in the event of an insured event and the price of insurance that the policyholder will pay to the insurer.

LIST OF REFERENCES

[1] AIG. (2020) *Cyber Insurance Summarized Assessment Report, American International Group, Inc.* [online]. Available from: www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyber-summarized-assessment-report-sample.pdf [Accessed 24 June 2021].

[2] Author not specified. *Say hello to HMM Algericas, the largest container vessel on earth* , [online] Shipping and Freight Resource, [online]. Available from: https://www.shippingandfreightresource.com/hmm-algericas-largest-container-vessel-on earth [Accessed 15 October 2021].

[3] Barki, D. and Deleze-Black, L. (ed.) (2020) Developments in International Seaborn Trade. *UNCTAD Review of Maritime Transport* 2020.

[4] Barlatier, J. (2020) Criminal Investigation and Criminal Intelligence: Example of Adaptation in the Prevention and Repression of Cybercrime. *Risks*, 8 (99), [online]. Available from https://doi.org/10.3390/risks8030099 [Accessed 23 June 2021].

[5] Bentley, M., Stephenson, A., Toscas, P., Zhu, Z. (2020) A Multivariate Model to Quantify and Mitigate Cybersecurity Risk, *Risks*, 8 (61), [online]. Available from https://doi.org/10.3390/risks8020061 [Accessed 24 June 2021].

[6] *BIMCO Guidelines on Cybersecurity Onboard Ships* (version 4, 2020).

[7] Burkacky, O., Deichmann, J., Klein, B., Pototzky, K., Scherf, G. (2020) *Cybersecurity in automotive: Mastering the challenge, report*, McKinsey&Company, [online]. Available from:www.mckinsey.com/industries/automotive-and-assembly/ourinsights/cybersecurit y-in-automotive-mastering-the-challenge# [Accessed 24 June 2021].

[8] Capra, G. S.: Protecting Critical Rail Infrastructure. The Counterproliferation Papers, *Future Warfare Series No. 38*, USAF Counterproliferation Center.

[9] CYRail Consortium Members. CYRail Recommendations on cybersecurity of rail signaling a communication systems. *UIC-ETF*, September 2018.

[10] Daily, J. et al. (2016) Towards a Cyber Assurance Testbed for Heavy Vehicle Electronic Controls. *SAE International Journal of Commercial Vehicles*, 9 (2).

[11] David, J. (2021) Cyber Attack on Railways in the Czech Republic. *Railtarget*, 22 March [online]. Available from: https://www.railtarget.eu/news/cyber-attack-on-railways-in-the-czech-republic-215.html [Accessed 24 June 2021].

[12] DiRenzo, J. et al. (2015) *The Little-known Challenge of Maritime Cybersecurity.* [online]. Available from: http://archive.dimacs.rutgers.edu/People/Staff/froberts/Maritime CyberCorfuPaper.final.pdf [Accessed 4 January 2021].

[13] Dobiáš, P. (2019) Kybernetická bezpečnost v mezinárodní přepravě se stále podceňuje, *Logistika* 25 (1).

[14] DPA/AFP.(2015) Hackers break into Lufthansa customer database. *Deutsche Welle,*10 April, [online]. Available from https://www.dw.com/en/hackers-break-into-lufthansa-customer-database/a-18374698 [Accessed 25 June 2021].

[15] Egan, R. et al. (2019) Cyber operational risk scenarios for insurance companies. *British Actuarial Journal,* 24, e6.

[16] EIOPA. Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies. *EIOPA*, 2. 8. 2018.

[17] Eling. M., McShane, M., Nguyen, T. (2021) Cyber risk management: History and future research directions. *Risk Management and Insurance Review,* 24, [online]. Available from: www.onlinelibrary.wiley.com/doi/epdf/10.1111/rmir.12169 [Accessed 25 June 2021].

[18] Forbes, V., L. (2018) *The Global Maritime Industry Remains Unprepared for Future Cybersecurity Challenges.* [online]. Available from: www.futuredirections.org.au/publication/the-global-maritime-industry-remains-unprepared-for-future-cybersecurity-challenges/ [Accessed 4 January 2021].

[19] Goldbaum, Ch., Rashbaum, W. K. (2021) The M.T.A. Is Breached by Hackers as Cyberattacks Surge. *New York Times*, 2 June [online]. Available from: https://www.nytimes.com/2021/06/02/nyregion/mta-cyber-attack.html [Accessed 24 June 2021].

[20] Goward, D. (2017) *Mass GPS Spoofing Attack in Black Sea?* [online]. Available from: www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea [Accessed 26 November 2021].

[21] Greenberg, A. (2016) Hackers Fool Tesla S'S Autopilot to Hide and Spoof Obstacles. [online] *New York: Wired.* Available from: www.wired.com/2016/08/hackers-fool-tesla-ss-autopilot-hide-spoof-obstacles [Accessed 4 January 2021].

[22] Hahn, D., A., Munir, A., Behzadan, V. (2021) Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges, I*EEE Intell. Transp. Syst. Mag*., 13 (1).

[23] Hambling, D. (2017) Ships fooled GPS spoofing attack suggests Russian cyberweapon, *New Scientist* [online]. Available from: www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/ [Accessed 4 November 2021].

[24] Harvey, J., Kumar, S. (2020) *A Survey of Intelligent Transportation Systems Security: Challenges and Solutions, Conference paper*, May 2020, [online]. Available from: https://www.researchgate.net/publication/342405096 [Accessed 10 November 2021].

[25] IATA. *Situational Analysis, Introduction to Cybersecurity Threats, Cybersecurity Mitigation Practices, Setting Up a Management System, Risk Assessment and Prioritization Instructions*, 2nd edition, IATA, effective as of June 2015.

[26] IATA. *Compilation of Cybersecurity Regulations, Standards, and Guidance Applicable to Civil Aviation*, Edition 2.0, April 2021.

[27] ICAO Working paper, Assembly – 39 Session, Executive Committee, Agenda Item 16: *Aviation Security – Policy, Addressing Cybersecurity in Civil Aviation*, A39-WP/17 EX/5, 30. 5. 2016.

[28] ICAO, *Aviation Cybersecurity Strategy*, Quebec, October 2019, p. 2 – 4.

[29] ICAO Working paper, Assembly – 40 Session, Executive Committee, Agenda Item 12: *Aviation Security – Policy, ICAO Cybersecurity strategy*, A40-WP/28 EX/13, 25. 6. 2019.

[30] *IMO Guidelines on Maritime Cyber Risk management* (IMO's Maritime Safety Committee, MSC-FAL.1/Circular 3, 5. 7. 2017).

[31] Irwin, L. (2021) 2020 cyber security statistics, *IT Governance* [online]. Available from: www.itgovernance.co.uk/blog/2020-cyber-security-statistics [Accessed 24 June 2021].

[32] Jirásek, P., Novák, L., Požár, J. (2015) *Výkladový slovník kybernetické bezpečnosti,* Prague: PA CR in Prague, Czech branch of AFCEA.

[33] Jirovský, V. (2007) Kybernetická kriminalita. Prague: Grada.

[34] Karfíková, M. et al. (2018) *Insurance Law.* Prague: Leges.

[35] Kessler, G. C., Craiger, J. P., Haas, J. C. (2018) Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System, *TransNav*.

[36] Kilcarr, S. (2015) Battling a hack: One fleet's story. *Fort Atkinson: Fleetowner.* [online]. Available from: https://www.fleetowner.com/technology/article/21692058/battling-a-hack-one-fleets-story [Accessed 4 January 2021].

[37] Kolouch, J., Bašta, P. et al. (2019) Kybernetická bezpečnost. Prague: CZ.NIC.

[38] Kure, H. I., Islam, S., Razzaque, M. A. (2018) An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. *Applied Sciences,* 8 (6) [online]. Available from: www.mdpi.com/2076-3417/8/6/898 [Accessed 25 June 2021].

[39] Lévy-Bencheton, C., Darra, E. (2015) *Cybersecurity and Resilience of Intelligent Public Transport, Good practices and recommendations,* Athens: ENISA.

[40] MacGregor, L. (2019) British Airways faces largest ever data breach fine for 2018 hack. *New Scientist and Press Association.* 8 July. [online]. Available from: https://www.newscientist.com/article/2208964-british-airways-faces-largest-ever-data-breach-fine-for-2018-hack/ [Accessed 25 June 2021].

[41] Mearian, L. (2015) Firewalls can't protect today's connected cars, *Computerworld* [online]. Available from: www.computerworld.com/article/2951878/telematics/firewalls-cant-protect-todays-connected-cars.html [Accessed 4 January 2021].

[42] Mecheva, T., Kanakov, N. (2020) Cybersecurity in Intelligent Transportation Systems, *Computers,* 9, 83, p. 6-8 [online]. Available from: www.mdpi.com/journal/computers [Accessed 10 November 2021].

[43] Morán Blanco, M., S. (2017) La Ciberseguridad y el uso de las tecnologías de la información y la comunicación (TIC) por el terrorismo. *Revista Española de Derecho International*, 69 (2).

[44] Muccin, E. (2015) *Combatting Maritime Cybersecurity Threats.* [online]. Available from: http://magazines.marinelink.com/Magazines/MaritimeReporter [Accessed 4 January 2021].

[45] Nurse, J., R., C., Axon, L., Erola, A., Agrafiotis, I., Goldsmith, M., Creese, S. (2020) *The Data that Drives Cyber Insurance: A Study into the Underwriting and Claims Processes, Conference Paper,* p. 3 [online]. Available from: https://www.researchgate.net/publication/340849886_The_Data_that_Drives_Cyber_Insurance_A_Study_into_the_Underwriting_and_Claims_Processes/link/5f521074a6fdcc9879ca0a2d/download [Accessed 24 June 2021].

[46] Oxera. (2020) The value of cyber insurance to the UK economy, *Oxford: Oxera Consulting LLP*, [online]. Available from: www.oxera.com/insights/reports/the-value-of-cyber-insurance-to-the-uk-economy/ [Accessed 23 June 2021].

[47] Page, C. (2021) Air India Data Breach: Hackers Access Personal Details Of 4.5 Million Customers. *Forbes*, 23 May [online]. Available from: https://www.forbes.com/sites/carlypage/2021/05/23/air-india-data-breach-hackers-access-personal-details-of-45-million-customers/ [Accessed 25 June 2021].

[48] Quingley, K., Roy, J. (2011) Cyber-Security and Risk Management in an Interoperable World An Examination of Governmental Action in North America, *Social Science Computer Review.* 30 (1) [online]. Available from: http://ssc.sagepub.com/content/30/1/83 [Accessed 24 June 2021].

[49] Romanosky, S., Ablon, L., Kuehn, A., Jones, T. Content analysis of cyber insurance policies: how do carriers price cyber risk? *Journal of Cybersecurity,* 5 (1) [online]. Available from: https://doi.org/10.1093/cybsec/tyz002 [Accessed 23 June 2021].

[50] Saul, J. (2017): Global shipping feels fallout from Maersk cyber attack. [online] *Thomson Reuters.* Available from: https://www.reuters.com/article/us-cyber-attack-maersk/global-shipping-feels-fallout-from-maersk-cyber-attack-idUSKBN19K2LE/ [Accessed 1 January 2021].

[51] Smejkal, V. (2018) *Kybernetická kriminalita*. 2nd ed. Pilsen: Aleš Čeněk.

[52] Svilicic, B., Brčić, D., Žuškin, S, Kalebić, D. (2019) Raising Awareness on Cyber Security of ECDIS, *TransNav*, 13 (1).

[53] Šulc, V. (2018) *Kybernetická bezpečnost.* Pilsen: Aleš Čeněk.

[54] The Nautical Institute. Charging your phone on the bridge? Think again!, *The Navigator,* June 2016.

[55] Tonn, G., Kesan, J. P., Czajkowski, J. and Zhang, L. (2018) *Cyber Risk and Insurance for Transportation Infrastructure*. [online]. Available from: https://riskcenter.wharton.upenn.edu/wp-content/uploads/2018/03/WP201802_Cyber-Security-Transportation-Sector.pdf [Accessed 4 January 2021].

[56] Ulianov, C., Hyde, P., Shaltout, R. E. (2018) Railway Applications for Monitoring and Tracking Systems. In: Marin Marinov (ed.) *Sustainable Rail Transport, Lecture Notes in Mobility*, Cham: Springer International Publishing.

[57] U. S. Department of Transportation. (2019) *Cybersecurity and Intelligent Transportation System, Best Practice Guide* – September 17, 2019, Publication Number: FHWA-JPO-19-

763, p. 35. [online] Available from: www.its.dot.gov/index.htm [Accessed 10 November 2021].

[58] Walker, J. (2018) *Autonomous Ships Timeline – Comparing Rolls-Royce, Kongsberg, Yara and More,* [online]. Available from: www.techemergence.com/autonomous-ships-timeline [Accessed 4 January 2021].

[59] Wares, S., Thompson, V. (2015) *Marsh Insights: Cyber Risk in the Transportation Industry,* p. 1, [online]. Available from: https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/Cyber%20Risk%20in%20the%20Transportation%20Industry-03-2015.pdf [Accessed 4 January 2021]

[60] Weise, E. (2015) *Officials look into whether hacker really took over plane*. USA Today, 17 May. [online]. Available from: https://eu.usatoday.com/story/tech/2015/05/17/hacker-sideways-chris-roberts-fbi-united/27492409/ [Accessed 21 June 2021].

[61] Which. (2021) Popular connected cars from Ford and Volkswagen could put your security privacy and safety at risk, *Which? Finds, Which* [online]. Available from: https://press.which.co.uk/whichpressreleases/popular-connected-cars-from-ford-and-volkswagen-could-put-your-security-privacy-and-safety-at-risk-which-finds/ [Accessed 26 November 2021].

[62] Wrede, D., Stege, T., Graf von der Schulenburg, J.-M. (2020) Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market. T*he Geneva papers on Risk and Insurance – Issues and Practice*, 45 (4) [online]. Available from: www.repo.uni-hannover.de/handle/123456789/10772 [Accessed 24 June 2021].

DOI 10.5817/MUJLT2022-1-2

THE RIGHT TO PRIVACY AND PROTECTION OF PERSONAL DATA: EMERGING TRENDS AND IMPLICATIONS FOR DEVELOPMENT IN JURISPRUDENCE OF EUROPEAN COURT OF HUMAN RIGHTS

by

YULIIA KOVALENKO*

The emergence of the right to personal data protection is usually considered in close proximity to the right to private life, however, the two rights despite the sufficient degree of similarity are not identical. The article analyses the main concepts and discussions around the protection of privacy and personal data protection, which primarily was only perceived as another facet of privacy, as well as provides a comprehensive overview of theoretical and practical problems associated with their protection. Provided for the right to data protection is not explicitly mentioned in the ECHR the main concern, therefore, is whether it receives an adequate level of protection within the Convention system. The article argues that given the lack of an explicit criterion for distinguishing the rights to privacy and data protection, it is the jurisprudence of the ECHR, which is of the utmost importance for the development of the right to personal data protection as a fundamental right. Due regard is given to the evolution of the fundamental approaches of the ECHR in this field. It is concluded that the effective enjoyment of the right to data protection, which is not specified in the text of the ECHR or its Protocols, undeniably relies on the ECHR's interpretation of the key data protection standards enlisted in the Convention no. 108, as well as relevant EU legislation.

* yuliiakovalenko108@gmail.com, PhD student of International and Comparative Law Department, Koretsky Institute of State and Law of National Academy of Sciences of Ukraine, Kyiv, Ukraine.

KEY WORDS
Privacy, Data protection, The right to private life, The right to personal data protection, ECHR.

1. INTRODUCTION

For a long time, personal data protection has only been considered as an aspect of the right to respect for private life, which is inextricably linked to the protection of other fundamental human rights and freedoms. However, the issue of data protection has drastically gained its importance with the unrestrained development of information technology. Accordingly, the question of determining the right to personal data protection and the standards of its protection becomes a modern challenge.

Since the middle of the XX century, the number of international human rights treaties enshrined the right to respect for private life as one of the fundamental human rights. First and foremost, the right to respect for private life was enshrined in Article 12 of the Universal Declaration of Human Rights of 1948, which set forth the list of fundamental human rights and is considered to be a 'milestone document', but yet is not legally binding. The rights incorporated in the Universal Declaration of Human Rights were further detailed in international treaties and other human rights instruments. The International Covenant on Civil and Political Rights of 1966 provided for the right to private life in Article 17 and the UN Human Rights Committee has been established to oversee its fulfilment and adherence. Furthermore, the right to respect for private life was guaranteed under Article 8 of the European Convention on Human Rights and Fundamental Freedoms of 1950 (hereinafter – the ECHR or the Convention).[1] Despite the fact that the right to respect for private life was already recognized as a fundamental human right, the provisions on the protection of privacy were formulated in such a general way that they did not detail certain aspects of personal data protection. Therefore, the issues related to personal data were considered only as an essential part

[1] Council of Europe, European Court of Human Rights, European Data Protection Supervisor, European Union Agency for Fundamental Rights (2018) *Handbook on European data protection law*. 2018 ed. Luxembourg: Publication Office of the European Union, pp. 18-27; Bygrave A. L. (2010). Privacy and Data Protection in an International Perspective. *Scandinavian studies in law*, pp. 181-183.

of the right to privacy, thus, the scope of personal data protection was sufficiently narrowed.

It was not until the second half of the XX – early XXI century that the active implementation of modern technologies in public and private spheres has led to a change of the approach to the recognition of the right to protection of privacy in connection with the processing of personal data. Due to the active use of cutting-edge technology, and the growing importance of the trans-border flow of personal data, the right to the protection of personal data began to be considered an independent right. Consequently, the UN Human Rights Committee issued General Comment no. 16 concerning the right to privacy providing particular attention to the protection of personal data and specifying that the rights of a person whose data was collected to ascertain what data was collected and to rectify or eliminate the incorrect or unlawfully obtained data. The UN Human Rights Committee also stressed that the right to privacy guaranteed under Article 17 extends both to the interference of the state authorities as well as natural and legal persons, however, originally right to respect for privacy only extended to the vertical relations with a state.[2] Likewise, the right to the protection of personal data was more comprehensively set forth by the Council of Europe in Convention no. 108 On the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter – Convention no. 108). It is noteworthy that Convention no. 108 is the first international binding treaty that establishes the definition of personal data and outlines key principles of data processing. In order to reinforce and strengthen the data protection with regard to the challenges of the digital age, Convention no. 108 has been modernized by protocol amending its provisions.[3]

It is worth mentioning that within the EU right to personal data protection was detailed in the Directive 95/46/EC of 24 October 1995, the Charter of Fundamental Rights of the EU, which after the entry into force of the Lisbon Treaty recognized the right to protection of personal

[2] UN Human Rights Committee (HRC) (1988). *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April. Available from: https://www.refworld.org/docid/453883f922.html [Accessed 11 January 2021].

[3] Council of Europe (2018). *Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* 10 October. Available from: https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a [Accessed 12 January 2021].

data as a fundamental right within the EU legal system, and the most recently adopted Regulation (EU) 2016/679 of 27 April 2016 usually referred to as GDPR.[4]

Nevertheless, public international law considers the status of personal data protection with continuing uncertainty given that: 1) the international human rights treaties ensures protection of private life in a broad manner and do not specify the particularities of data protection rights; 2) other international instruments concerning data protection are either regional or are non-binding; 3) there is a lack of international consensus on the scope of privacy and data protection given the differences in cultural and legal perceptions; 4) the substantial fragmentation on data protection in national and regional legal systems. It is alleged that future developments of data protection in international law could be achieved by either developing a uniform international treaty or using the experience of UNCITRAL to the data protection issues.[5] Currently, the only binding international treaty is Convention no. 108, which was adopted by the Council of Europe, yet it could be acceded by non-European countries. Although, it is argued that Convention no. 108 should be adopted by the UN as a global treaty given that it has already been accessed by countries outside the Council of Europe and therefore has all potential to be adopted as a global data protection treaty.[6]

There is no doubt that the full range of aspects related to the right to data protection and the definition of the principles of data protection are gradually developing through court interpretation. The significant impact both on the development of the right to personal data protection and the improvement of the legal framework governing the protection

---

[4] European Commission (2018) *Data Protection in the EU*. [online]. Available from: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en [Accessed 15 January 2021].

[5] Kittichaisaree K., Kuner C. (2015) The Growing Importance of Data Protection in Public International Law. *EJIL:Talk!* 14. Available from: https://www.ejiltalk.org/the-growing-importance-of-data-protection-in-public-international-law/ [Accessed 25 January 2021].

[6] Greenleaf G. (2018) The UN should adopt Data Protection Convention 108 as a global treaty: Submission on 'the right to privacy in the digital age' to the UN High Commission for Human Rights, to the Human Rights Council, and to the Special Rapporteur on the Right to Privacy. Sydney, 8 April 2018. Available from: https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/GrahamGreenleafAMProfessorLawUNSWAustralia.pdf [Accessed 13 January 2021]; Buttarelli G. (2016) Convention 108: from a European Reality to a Global Treaty. *Council of Europe International Conference*, Strasbourg, 17 June. Available from: https://edps.europa.eu/sites/edp/files/publication/16-06-17_speech_strasbourg_coe_en.pdf [Accessed 29 January 2021].

of personal data is made by the European Court of Human Rights (hereinafter – the ECHR or the Court). Moreover, since Convention no. 108 does not envisage the judicial or other controlling body to oversee compliance with its provisions, to some extent, it is the ECHR that may be treated as such a controlling body, which reviews the cases related to an alleged violation of the right to privacy under the Convention and take into account the provisions of the Convention no. 108.[7] That is being so the Court also pay particular attention not only to the domestic law and practice of the state concerned but also to the relevant international legal acts, EU law, as well as jurisprudence in the field of the data protection, including the case-law of the Court of Justice of the EU. Thus, the ECHR practice is of the utmost importance for the consolidation and streamlining of the data protection principles and standards.

2. RIGHT TO PRIVACY AND PERSONAL DATA PROTECTION UNDER THE ECHR: GENERAL ASPECTS

Traditionally privacy extends to the confidentiality of communications, covers the secrecy of telephone conversations, e-mails, and other forms of communication, including personal data on the Internet. At the same time, the category of personal data as information on an identified or identifiable individual covers not only printed textual information such as an individual's name, address, date of birth, identification card number, and phone number, but also photos, videos, and voice samples, even if recorded in public places and may also include confidential personal information about one's family life.[8] Privacy within the European legal framework covers the protection of an individual's 'personal space' that goes beyond data protection, therefore, privacy can be considered as a concept which is both broader than and independent from data protection, though there can be a significant overlap between the two.[9]

Turning to the ECHR, the cases regarding the violation of the right to protection of personal data are examined in terms of Article 8 of the Convention, which ensures the right to respect for private

[7] Rojszczak M. (2020) Does Global Scope Guarantee Effectiveness? Searching for a New Legal Standard for Privacy Protection in Cyberspace. *Information & Communications Technology Law*, 29 (1), p. 30.

[8] Pazyuk A. (2016) European Approach to the Data Protection in the Police Sector: Current Status and Trends. *Law Review of Kyiv University of Law*, 4, p. 360.

[9] Kuner C. (2009) An International Legal Framework for Data Protection: Issues and Prospects. *Computer Law & Security Review*, 25, p. 313.

life. The protection of privacy under Article 8 originally was focused on protection from interference by public authorities, omitting the possible breaches in the private sphere. Although Article 8 provided for a negative obligation of the state and therefore privacy was originally granting negative freedom to individuals in relation with a state, yet the Court subsequently diverged from the initial focus of the Convention authors by accepting both positive obligations for states and positive freedom to individuals.[10]

The right to personal data protection was not initially incorporated within the text of the ECHR as an independent right. Moreover, the Convention from the outset was not perceived as an instrument for adequate protection of personal data since the latter developed after the adoption of the Convention and a special international treaty to regulate this sphere was further developed. Yet the ECHR contributed significantly to the evolution of the data protection concept by providing a broad interpretation of the right to respect for private life and defining the limits of Article 8 of the Convention.

Being of the multifaceted nature, needless to say, that private life under Article 8 of the Convention "*is a broad term not susceptible to exhaustive definition*".[11] In this regard, for a while, the issue of personal data protection was considered only in a close connection to the right to private life. Hence, the ECHR has been steadily developing the scope of the right to private life and has respectfully interpreted different aspects of personal data protection. However, it was only after the decision in *Tyrer v. the United Kingdom* case in 1978 that the Court had accepted the living instrument doctrine, which implies that "*the Convention is a living instrument which must be interpreted in the light of present-day conditions*".[12] Upon adoption of the *Tyrer* decision, the Court for the first time had recognized that the provisions of the Convention must be interpreted dynamically and reflect the current realities, challenges, and threats of a changing environment. For these reasons, the rights and freedoms listed in the Convention in order to be "*practical and effective, not theoretical and illusory*" should not be deemed as exhausted.[13] The living instrument

[10] Van der Sloot B. (2014) Privacy as Human Flourishing: Could a Shift Towards Virtue Ethics Strengthen Privacy Protection in the Age of Big Data? *JIPITEC,* 5(3), pp. 230-231.

[11] *Peck v. the United Kingdom* (2003) No. 44647/98, § 57, ECHR 2003-I.

[12] *Tyrer v. the United Kingdom* (1978) No. 5856/72, § 31, ECHR, Series A no. 26.

[13] *Airey v. Ireland* (1979) No. 6289/73, § 24, ECHR, Series A no. 32.

doctrine primarily has had its effect on the provisions of Article 8 of the ECHR. Having functioned as the main reference when the Court accepts new rights and freedoms under the Convention, Article 8 of the ECHR subsequently extended its scope and guaranteed the right to data protection.[14]

Nonetheless, the right to data protection is related to, yet it differs from the right to private life. While the right to data protection is always connected to the information on the identified or identifiable individual, the right to privacy does not necessarily include it. However, privacy is of a wider perspective that embodies a set of rights and values, including the right to be let alone, intimacy, autonomy, personhood, etc.[15] It is also worth mentioning that the scope of data protection is broader than the scope of privacy since not only does it cover the information on the identified individual but also all information on the identifiable individual, which includes a sufficiently wider variety of the information. Another difference concerns the responsibilities of private parties: while the right to privacy mainly addresses the obligations of public authorities not to interfere and to adopt the laws to secure relations between individuals, the right to data protection imposes quite identical obligations on both the authorities and private parties such as, for instance, employers or service providers.[16] Furthermore, it is also asserted that the right to data protection offers individuals more control over different types of data than the right to privacy. Thus, personal data protection is to be considered as a right that greatly coincides with the right to privacy still ensuring complementary, distinct benefits for individuals. While considering the cases related to personal data protection, the Court gives due importance to whether the individual is identified or identifiable. The latter issue reflects the sphere of application of the data protection legislation with regard to the definitions of 'personal data', which is broader than the concept of 'privacy interference' under Article 8.[17]

---

[14] Van der Sloot B. (2015) Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data". *Utrecht Journal of International and European Law*, 31(80), pp. 39 -40.

[15] Tzanou M. (2013) Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a not so New Right. *International Data Privacy Law,* 3(2), pp. 89-93.

[16] Kokott J., Sobotta C. (2013) The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, 3(4), pp. 224-226.

The advance of modern technologies makes the collection, storing, processing, and disclosure of personal data a vital part of day-to-day life, leading to the emergence of the right to data protection. Even though not initially foreseen in the text of the Convention, the right to data protection found its rightful place within the Convention system. Currently, the right to data protection, despite being closely connected to the right to privacy, is receiving its growing independence.

3. THE ECHR APPROACHES TOWARDS PROTECTION OF PERSONAL DATA

In order to assess the adequacy of personal data protection under the Convention system, the concepts applied by the Court should be analyzed, inter alia, in the light of the key data protection standards, with due regard to the inexhaustible nature of the 'personal data' and specificity of the sensitive data protection.

The ECHR has been gradually confirming that personal data protection, by and large, comes within the scope of Article 8 of the Convention. In the 1980s, a new doctrine originated in the ECHR case-law requiring that the laws should be accessible and foreseeable. At the outset, the Court hesitantly applied this doctrine to the right to privacy and protection of personal data matters, especially because these principles were difficult to uphold in cases of secret surveillance and special police investigations where secrecy and un-foreseeability are constitutive.[18] Nevertheless, this doctrine undeniably has influenced the path of data protection under the Convention. Hence the Court considers two aspects related to the data protection – the state's compliance with its positive obligations, i.e. guarantees of observance of the law, and negative obligations, i.e. refraining from arbitrary interference (and the sufficient safeguards in this respect). The Court also applies the margin of appreciation doctrine to the issues of data protection, providing a state with discretion in fulfilling its obligations under the Convention and reflecting its subsidiary role.[19]

---

[17] Lynskey O. (2014) Deconstructing Data Protection: the 'Added-Value' of a Right to Data Protection in the EU Legal Order. *International and Comparative Law Quarterly,* 63(3), pp. 581-583.

[18] Van der Sloot B. (2020) The Quality of Law: How the European Court of Human Rights Gradually Became a European Constitutional Court for Privacy Cases. *JIPITEC,* 11(2), p. 232.

[19] Byström N. (2016). The Data Subject and the European Convention on Human Rights: Access to Own Data. *EDILEX,* pp. 209-246.

The Court has been progressively introducing a broad interpretation of the term 'private life' with the equally broad notion of 'personal data' in data protection regulation.[20] Indeed, the scope of personal data is hard to be defined, and it includes not only ordinary personal data, such as name or date of birth but also other information that might lead to the identification of a person, including IP address, GPS data or DNA profile. In that respect, the Court also contributes to the interpretation of the key data protection principles, namely, the lawfulness, fairness and transparency, adequacy, relevance, and accuracy of personal data and the terms of its storage.

Since none of the international data protection documents contains an exhaustive list of what constitutes personal data, it is the Court's role to underline its inexhaustible nature and define whether certain information is personal data in each case. For instance, it did so in *Malone v. the United Kingdom* which related to the interception of communications of the applicant on behalf of the police by the metering of his telephone.[21] An important conclusion was reached that the use of data obtained from metering, including the numbers dialed, constitutes an integral element in the telephone communications and consequently it was stressed that the release of that information to the police without the consent of the subscriber was in violation of Article 8.[22] In this case, not only did the ECHR interpreted the scope of the 'personal data', by enlisting the information on dialled calls as information attributed to the individual, but also it significantly impacted the accessibility and foreseeability doctrine concerning privacy and existent data protection legislation.

Further, in *Benedik v. Slovenia, the* ECHR defined the scope of 'personal data' while dealing with the issue of obtaining data on the subscriber's dynamic IP address by the police. The Court pointed out that unlike the static IP address, which is permanently allocated to the device, a dynamic IP address is assigned temporarily, typically each time the device connects to the Internet. It was emphasized that the subscriber's

[20] de Hert P. and Gutwirth S. (2009) Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In: Gutwirth S., Poullet Y., de Hert P., Nouwt J., de Terwangne C. (eds.) *Reinventing Data Protection?* Dordrecht: Springer Science, p. 21.

[21] Metering is a process of registration of the numbers dialed, the time and duration of each call.

[22] *Malone v. the United Kingdom* (1984) No. 8691/79, §§ 83-84, ECHR, Series A no. 82 The ECHR practice on the interception of the telephone communications further developed in *Weber and Saravia v. Germany* (2006) No. 54934/00, ECHR 2006-XI and *Szabó and Vissy v. Hungary* (2016) No. 37138/14, ECHR.

information associated with the dynamic IP, including the address, was not publicly available and allowed the police to identify the home from which the Internet connections had been made and reveal the applicant's identity.[23] Thus, the Court enlisted dynamic IP address to personal data since it could lead to the identification of an individual. Moreover, the Court recognized that GPS information also constitutes personal data and its collecting and processing falls within Article 8 of the Convention, given that it may determine the whereabouts and movements of a person in the public sphere. [24]

It is to note that the Court pays particular attention to the processing of the sensitive personal data – namely, health-related data, data on racial or ethnic origin, political opinions, religious beliefs, genetic and biometric data or information on a person's sex life or sexual orientation – and carefully examines such cases since this data needs a higher level of protection due to its sensitive nature. For instance, the case of *Z. v. Finland* related to the seizure of medical records in the course of criminal proceedings, disclosure of information on HIV status by the press, and publication of the applicant's name and health condition in judgment, while *M.S. v. Sweden* related to the transfer of the applicant's medical records by the clinic to the Social Insurance Office. In both cases, the ECHR stressed that the protection of personal data, particularly medical data, is of fundamental importance to a person's enjoyment of the right to private life as guaranteed by Article 8. Moreover, disclosure of medical and health data may dramatically affect an individual's private and family life, as well as social and employment situation by exposing that person to opprobrium and the risk of ostracism. Respect for the confidentiality of such data is considered a vital principle, and it is of the utmost importance to provide appropriate safeguards to prevent any communication or disclosure of personal health data that could adversely affect the applicant's rights.[25] Also, landmark conclusions were reached in *P. and S. v. Poland* related to the dissemination by the hospital staff to the press sensitive personal data of the 14-year-old applicant, who

[23] *Benedik v. Slovenia* (2018) No. 62357/14, §§ 109, 113, ECHR.

[24] *Uzun v. Germany* (2010) No. 35623/05, §§51-52, ECHR 2010; On the surveillance and use of the GPS data see *Ben Faiza v. France* (2018) No. 31446/12, ECHR.

[25] *Z. v. Finland* (1997) No. 22009/93, §§ 95-96, ECHR, Reports of Judgments and Decisions 1997-I; *M.S. v. Sweden* (1997) No. 20837/92, § 41, ECHR, Reports of Judgments and Decisions 1997-IV.

became pregnant as a result of rape and decided to have an abortion. Even though the information released to the public did not contain the names or other details on the applicant, the Court noted that this information was detailed enough to establish the whereabouts and contact the applicant.[26] Thus, to fall within Article 8, the information concerning a person, even if published anonymized, must be detailed enough to establish the applicant's identity.

Meanwhile, it is acknowledged that the states enjoy wide discretion in the course of a criminal investigation and are authorized to collect sensitive personal data for relatively long periods. Yet the Court critically assess the data retention periods and requires data to be deleted once it is no longer relevant. It was *S. and Marper v. the United Kingdom* where the Court stated that the processing of DNA profiles allows the authorities to assess the likely ethnic origin of the donor and that such techniques are, in fact, used in police investigations. The prolonged storage by the authorities of the applicants' fingerprints, cell samples, and DNA profiles after the completion of the criminal proceedings and the use of this data to determine their ethnic origin had infringed and violated their rights.[27] Moreover, in *Gaughran v. the United Kingdom*, it was stressed that the state failed to strike a fair balance between the public and private interests at stake, given the indefinite retention of biometric data of the previously convicted individual, including his DNA profile, fingerprints, and photos in the absence of any reference to the seriousness of the offence or the continuing need for such unlimited retention and any safeguards to review or delete of such data.[28] Therefore, indefinite retention of personal data, especially storage of sensitive personal data, could lead to a disproportionate interference with the individual's rights and the provisions of domestic law on that matter must be precise and clear to guarantee diligence of the authorities.

Due regard is also given to the states' discretion to collect personal data by secret measures and its storage in the secret state registers, which are

---

[26] *P. and S. v. Poland* (2012) No. 57375/08, § 130, ECHR.

[27] *S. and Marper v. the United Kingdom* (2008) nos. 30562/04, ECHR, and 30566/04, §§ 76, 86, ECHR 2008. The ECHR findings on the storage of fingerprints were further outlined in *M.K. v. France* (2013) No. 19522/09, ECHR.

[28] *Gaughran v. the United Kingdom* (2020) No. 45245/15, §§ 96-97, ECHR. More on the use of data obtained from the video surveillance of public places see *Peck v. the United Kingdom* (2003) No. 44647/98, ECHR 2003-I; on a DNA saliva samples see *Dragan Petrović v. Serbia* (2020) No. 75229/10, ECHR.

highly intrusive and requires sufficient guarantees for the individuals. One of the first cases in this regard was *Leander v. Sweden*, where the Court analyzed the legality of maintaining secret police files with information on the private life of the applicant and assessing the applicant by using that information in the process of employment. Although no violation of Article 8 was found since the national security prevailed over the individual interests, the ECHR noted that the storage and distribution of information about an individual by public authorities along with their refusal to allow the individual to refute this information amounted to an interference with the right to privacy.[29] Consequently, in *Amann v. Switzerland*, which related to the application of the secret surveillance measures, the Court confirmed this approach. Particular attention was given to Convention no. 108 while assessing whether there was the interference of public authorities by collecting and processing of the applicant's personal data, namely interception of telephone conversations, creation, and storage of a file about a person in this regard. It was also stressed that in the context of personal data the term 'private life' must not be interpreted restrictively.[30]

Nonetheless, even public information, if it is systematically collected and stored in files held by the authorities, could fall within the scope of data protection. For instance, in *M.M. v. the United Kingdom*, which related to the criminal data recorded by the authorities, *the* Court concluded: 'the greater the scope of the recording system, and the greater the amount and sensitivity of data held and available for disclosure, the more important the content of the safeguards to be applied at the various crucial stages in the subsequent processing of the data'. The Court another time emphasized that it is the authorities responsible for retaining and disclosing criminal record data that have an obligation to secure respect for private life, which is particularly important given the nature of the data held and the potentially devastating consequences of their disclosure.[31]

The issues related to the right to the destruction of a personal data file, lawfulness of the processing of personal data even collected without the use of secret surveillance and storage of a file containing the applicant's personal data, including information on his public activities, publications,

---

[29] *Leander v. Sweden* (1987) No. 9248/81, § 48, ECHR, Series A no. 116.

[30] *Amann v. Switzerland* (2000) No.27798/95, §§ 61-67, ECHR 2000-II. See also the Court's findings in *Taylor-Sabori v. the United Kingdom* (2002) No. 47114/99, ECHR; *Dumitru Popescu v. Romania (no. 2)* (2007) No. 71525/01, ECHR.

[31] *M.M. v. the United Kingdom* (2012) No. 24029/07, § 200, ECHR.

participation in political organizations, etc., was scrutinized in the case *Rotaru v. Romania*. The ECHR concluded that national law did not specify the circumstances to collect information by the intelligence service, the type of information that may be stored, the categories of persons in respect of whom it may be collected, as well as the collection procedure itself. Besides, the legislation did not mention specific retention periods of such information, the range of persons who have access to the files, the manner in which the data may be used, and the nature of those files. The Court noted that the storage and usage of such information were not accompanied by safeguards against abuse of powers.[32] Given these facts, the Court found that the relevant Romanian legislation was not sufficiently clear and foreseeable.

Undoubtedly, the interests of national security could prevail over individual interests, yet the law must provide sufficient safeguards against arbitrariness. The summary of the data protection principles for information obtained by secret surveillance measures that allowed interception of telephone communication was held in *Roman Zakharov v. Russia*. It its judgement the ECHR has formulated detailed criteria on the data protection: 1) the data should be collected on the basis of law; 2) the provisions of the law meet the requirements of accessibility, clarity and foreseeability; 3) the decision on granting secret surveillance measures should be subject to judicial review or control by other body; 4) such control should provide an opportunity for the person to present his arguments; 5) the court decision must be substantiated to prevent arbitrary interference; 6) the instructions in the court decision as to which data (documents) could be accessed should be as clear as possible; 6) the person in respect of whom the data is collected secretly must have effective means of protection, which would provide for the possibility of challenging the legality and reasonableness of the decision on access to such information, as well as obtaining compensation in the event of a violation; 7) access should only be granted to information necessary for the purposes of the investigation; 8) the information obtained must be properly recorded, stored and protected in order to prevent its modification, illegal destruction and

[32] *Rotaru v. Romania* (2000) No. 28341/95, §§ 53-63, ECHR 2000-V. The Court's opinion on the data collected and stored in public register see also *Gardel v. France* (2009) No.5335/06, ECHR 2009; *Catt v. the United Kingdom* (2019) No. 43514/15, ECHR; on the data held in the secret state register see *Segerstedt-Wiberg and Others v. Sweden* (2006) No. 62332/00, ECHR 2006-VII; *Shimovolos v. Russia* (2011) No. 30194/09, ECHR.

dissemination; 9) the information should be destroyed immediately once there is no need in it.[33] Thus, failure to comply with these rules results in the violation of Article 8 of the Convention.

It is important that the rights of data subjects are widely interpreted by the Court, including the right to access the data file and the right to rectify or destruct such data. For instance, in *Gaskin v. the United Kingdom, the* ECHR considered a positive obligation of a state to ensure the right to access personal data given the restriction of the applicant's access to social services documents on his early childhood and upbringing. It was noted that the applicant's rights were infringed due to the lack of an independent body to deal with requests for access to his personal data file. Moreover, the ECHR stressed the importance of ensuring the confidentiality and protection of third-person data by providing a certain individual with access to his or her data.[34]

Besides, the Court gradually deviated from its standpoint that privacy concerns only the vertical relations and expanded the guarantees of Article 8 to the horizontal relationship between individuals themselves, for instance, in relations between employer and employee. An important aspect that should be considered in that respect is whether the individual could reasonably expect privacy and anonymity of his data. In *Bărbulescu v. Romania*, regarding the monitoring of the employee's e-mails and access to their content, the Court held that it is particularly important to guarantee the employee's reasonable expectation of the privacy of his communication even if made from the employer's computer. In that case, the ECHR defined six critical factors to be regarded by the employer in the case of introduction the monitoring measures over the employees' correspondence: 1) notification of the employee on the possibility of such monitoring; 2) the extent of monitoring by the employer and the degree of interference in the employee's privacy; 3) provision of the legitimate reasons to justify the monitoring and access to the content of communication by the employer; 4) the possibility to use other less

[33] *Roman Zakharov v. Russia* (2015) No. 47143/06, §§ 227-305, ECHR. The provisions on bulk interception of communication were considered in *Centrum För Rättvisa v. Sweden* (2018) No. 35252/08, ECHR, *Big Brother Watch and others v. the United Kingdom* (2018) Nos. 58170/13, 62322/14 and 24960/15, ECHR.

[34] *Gaskin v. the United Kingdom* (1989) No. 10454/83, § 49, ECHR, Series A no. 160. On the access to the file containing personal data were see also *Odièvre v. France* (2003) No. 42326/98, ECHR 2003-III; *K.H. and Others v. Slovakia* (2009) No. 32881/04, ECHR 2009; *Haralambie v. Romania* (2009) No. 21737/03, ECHR.

intrusive monitoring measures; 5) the consequences of monitoring for the employee; 6) adequate safeguards against the abuse for the employee.[35] In *Antovic and Mirkovic v. Montenegro, the* Court examined the issue of video surveillance in the university auditoriums where the applicants held their classes. This case highlights the existent distinction between the right to private life and the right to personal data protection. It was noted that the data collected by the video surveillance in the workplace, both secret and not, is of a considerable intrusion into the employee's private life.[36] Consequently, since data protection covers the processing of all information on an identified or identifiable individual, the video monitoring (and recording), even though it was impersonal to some extent due to the blurred character of the recordings, amounted to the processing of information of the identifiable individual.[37]

Interestingly, the ECHR also decided over the cases related to data protection in respect of the legal entities. While international data protection documents only concern the rights of individuals, it is to notice that within the Convention system legal entities are also entitled to such protection. In *Bernh Larsen Holding AS and Others v. Norway*, the tax authority ordered one of the applicants' companies to provide copies of all data from a computer server shared with the other two applicants-companies. The ECHR acknowledged that requiring such information from the applicants constitutes an interference with their rights under Article 8 of the Convention. Yet the Court stressed that the interference was based on the national law, which was accessible, sufficiently clear and foreseeable, and it was necessary in a democratic society. Moreover, the procedure at issue had been accompanied by effective and adequate safeguards: 1) the applicant was notified in advance about a possible tax audit; 2) the applicants' representatives were present and could immediately object to the interference; 3) the backup copy of the data was sealed and could only be open in the applicants' presence; 4) upon

[35] *Bărbulescu v. Romania* (2017) No. 61496/08, §§ 71-81, 121, ECHR. On contrary, monitoring measures introduced by public company were justified in *Libert v. France* (2018) No. 588/13, §§ 46, 52, ECHR.

[36] *Antović and Mirković v. Montenegro* (2017) No. 70838/13, §§ 55-56. More on secret video surveillance at work see *López Ribalda and Others v. Spain* (2019) Nos. 1874/13 and 8567/13, ECHR.

[37] Ivanišević B. (2018) Distinction Between Privacy and Data Protection in ECtHR's Montenegro Case. *BDK Advokati*. 13 February. Available from: https://bdkadvokati.com/distinction-between-privacy-and-data-protection-in-ecthrs-montenegro-case/ [Accessed 02 February 2021].

the completion of the tax audit all data and traces of its content was to be destroyed.[38] Thus, the Court concluded that a fair balance was struck between the applicants' rights and interest in protecting the privacy and data of employees, on the one hand, and the public interest in ensuring effective tax audits, on the other.

The Court recognized that some issues related to personal data protection might also raise issues under Article 10 of the Convention, which guarantees freedom of expression and access to information. The majority of cases before the Court concerning the relationship between those two rights are related to the publication of the material containing personal data. One of such cases is *Satakunnan Markkinaporssi Oy and Satamedia Oy v. Finland*, in which the newspaper published tax data on 1.2 million citizens, which amounted to a third of all taxable persons in Finland, most of whom were ordinary taxpayers and only a small part of them – people with high income, public figures or celebrities within the meaning of the Court's case law. The information published by the applicants' companies did not relate to a specific category of persons, such as politicians, public figures, civil servants, or other persons belonging to the public sphere through their activities or profits. However, the applicants relied on the relative anonymity of the published data by referring to the 'blending in' factor – the mass data was published, all in the same manner, so the information concerning a specific person 'blended in' and is anonymized to a certain extent. It was noted, however, that the applicants did not take into account the nature of the tax data since it was collected and published by the authorities for one purpose and by the applicants for a completely different. Though the personal data in question were public and the collection of information is an important preparatory step in journalistic activity and an integral, protected part of freedom of the press, yet the public interest in providing access to and collection of large amounts of tax data does not necessarily or automatically mean that there is also an interest in publishing this raw data without any analytical input.[39] Therefore, a distinction should be made between

[38] *Bernh Larsen Holding AS and Others v. Norway* (2013) No. 24117/08, §§ 106, 126-134, ECHR. Similarly, the search of the law firm's premises and seizure of the computer files and emails did not violate Article 8 in *Sérvulo & Associados - Sociedade de Advogados, RL and Others v. Portugal* (2015) No. 27013/10, ECHR.

[39] *Satakunnan Markkinaporssi Oy and Satamedia Oy v. Finland* (2017) No. 931/13, §§ 137, 175-181, ECHR. See also the Court's findings in *Axel Springer AG v. Germany* (2012) No. 39954/08, ECHR and *Annen v. Germany* (2015) No. 3690/10, ECHR.

the processing of information for journalistic purposes and the dissemination of raw data, to which journalists only provide 'privileged' access. In the Court's view, the publication of the data in the manner and to the extent that the applicant companies had done was not contributing to public discussion, nor was it intended to do so.

Another important decision was reached in *Segerstedt-Wiberg and Others v. Sweden* where the Court considered that the storage of personal data related to political opinion, affiliations and activities kept in the state register had been deemed unjustified for the purposes of Article 8 and constituted an unjustified interference with the rights protected by Articles 10 and 11.[40]

Thus, the Court's jurisprudence displays various issues related to data protection, defines the scope of the right to data protection, its categories and which operations constitute data processing. It is the evolutive doctrine that empowers the Court to define the scope of data protection in the light of the rapid technological development and the accessibility and foreseeability doctrine that serve as the basis for judicial interpretation of the rights of the data subjects as well as core principles of data protection. Yet certain consideration arises while balancing the reasonable expectations of privacy and distinct rules for data protection. Even though the rights to privacy and personal data protection significantly overlap, still they should not be deemed virtually the same. It is evident from the recent Court's case-law that the difference between the two rights exists, and it is the Court's role to provide specific, distinct requirements for data protection.

4. CONCLUSION

Data protection from the outset of its emergence has been related to privacy to such an extent that it was complicated to establish precisely not only its notion but also its scope and unprecedented value. The fragmentation of data protection is attributed to the lack of a global international treaty or another relevant instrument in this sphere. In this regard, the main issue is whether the right to data protection receives adequate degree of protection under the Convention system since it is not explicitly mentioned either in the Convention or its Protocols. This article reveals

[40] *Segerstedt-Wiberg and Others v. Sweden* (2000) No. 62332/00, §§ 90-92, 107, ECHR 2006-VII.

the main concepts the Court applies in data protection cases. By applying the data analysis and comparative methods, the conclusion is reached that the ECHR has been contributing to the development of this right by defining the key principles of data protection which correspond to the underlying standards stemming from international legal acts in this sphere, including Convention no.108 and relevant EU data protection legislation. Accordingly, the Court has established that personal data should only be collected in accordance with the law, for specific and legitimate purposes, and it is the obligation of the states to establish adequate, accessible and sufficiently foreseeable data protection legislation. It is also important that a fair balance is struck between the aim of collection, processing, storage, or disclosure of data and the impact it has on the individual's rights.

The ECHR cases examined in the article confirm that the inexhaustible nature of the 'personal data' requires the Court to progressively broaden the scope of the latter in light of new technological developments and present-day conditions. Following the Court's case-law it is certain that the personal data by its definition is broader than the interests safeguarded by the scope of the right to private life. Thus, the right to data protection being emerged from the right to privacy is linked to the latter but is rather distinct. The Court's jurisprudence, hence, serves two key purposes – firstly, it fosters the development of the right to data protection, and secondly, it provides the consistency in interpretation of the key data protection principles and rights of data subject with regard to the modern challenges. Even not directly specified under the Convention system, the right to data protection is safeguarded by the Court and successively increasing its independence and significance as a fundamental right. This article concludes, however, that there is a continuing need to recognize the right to data protection as autonomous within the Convention system, which will provide a sufficiently higher level of protection for the data subject, including the specificities of data protection defined in the relevant international standards and will allow finding its rightful place in the existing human rights framework.

LIST OF REFERENCES

[1] *Airey v. Ireland* (1979) No. 6289/73, ECHR, Series A no. 32.

[2] *Antović and Mirković v. Montenegro* (2017). No. 70838/13, ECHR.

[3] *Amann v. Switzerland* (2000). No. 27798/95, ECHR 2000-II.

[4] *Bărbulescu v. Romania* (2017) No. 61496/08, ECHR.

[5] *Benedik v. Slovenia* (2018) No. 62357/14, ECHR.

[6] *Bernh Larsen Holding AS and Others v. Norway* (2013) No. 24117/08, ECHR.

[7] Buttarelli G. (2016) Convention 108: from a European reality to a global treaty. *Council of Europe International Conference*, Strasbourg, 17 June 2016. Available from: https://edps.europa.eu/sites/edp/files/publication/16-06-17_speech_strasbourg_coe_en.pdf [Accessed 29 January 2021].

[8] Bygrave A. L. (2010). Privacy and Data Protection in an International Perspective. *Scandinavian studies in law,* pp. 181-183.

[9] Byström N. (2016). The Data Subject and the European Convention on Human Rights: Access to Own Data. *EDILEX,* pp. 209-246.

[10] Council of Europe (2018). *Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* 10 October. Available from: https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a [Accessed 12 January 2021].

[11] Council of Europe, European Court of Human Rights, European Data Protection Supervisor, European Union Agency for Fundamental Rights (2018) *Handbook on European data protection law*. 2018 ed. Luxembourg: Publication Office of the European Union, pp. 18-27.

[12] de Hert P. and Gutwirth S. (2009) Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In: Gutwirth S., Poullet Y., de Hert P., Nouwt J., de Terwangne C. (eds.) *Reinventing Data Protection?* Dordrecht: Springer Science, pp. 3-44.

[13] European Commission (2018) *Data Protection in the EU*. [online]. Available from: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en [Accessed 15 January 2021].

[14] *Gaskin v. the United Kingdom* (1989). No. 10454/83, ECHR, Series A no 160.

[15] *Gaughran v. the United Kingdom* (2020). No. 45245/15, ECHR.

[16] Greenleaf G. (2018) 'Modernised' data protection Convention 108+ and the GDPR. 154 *Privacy Laws & Business International Report* 22-3. Available from: http://www.ssrn.com/link/UNSW-LEG.html [Accessed 13 January 2021].

[17] Ivanišević B. (2018) Distinction Between Privacy and Data Protection in ECtHR's Montenegro Case. *BDK Advokati*. 13 February. Available from:

https://bdkadvokati.com/distinction-between-privacy-and-data-protection-in-ecthrs-montenegro-case/ [Accessed 02 February 2021].

[18] Kittichaisaree K., Kuner C. (2015) The Growing Importance of Data Protection in Public International Law. *EJIL:Talk!* 14 October. Available from: https://www.ejiltalk.org/the-growing-importance-of-data-protection-in-public-international-law/ [Accessed 25 January 2021].

[19] Kokott J., Sobotta C. (2013) The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, 3(4), pp. 222–228.

[20] Kuner C. (2009) An International Legal Framework for Data Protection: Issues and Prospects. *Computer Law & Security Review*, 25, pp. 307-317.

[21] *Leander v. Sweden* (1987) No. 9248/81, ECHR, Series A no. 116.

[22] Lynskey O. (2014) Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order. *International and Comparative Law Quarterly,* 63(3), pp. 569-597.

[23] *M.M. v. the United Kingdom* (2012). No. 24029/07, ECHR.

[24] *M.S. v. Sweden* (1997). No. 20837/92, ECHR, Reports of Judgments and Decisions 1997-IV.

[25] *Malone v. the United Kingdom* (1984) No. 8691/79, ECHR, Series A no. 82.

[26] *P. and S. v. Poland* (2012). No. 57375/08, ECHR.

[27] *Panteleyenko v. Ukraine* (2006). No. 11901/02, ECHR.

[28] Pazyuk A. (2016) European Approach to the Data Protection in the Police Sector: Current Status and Trends. *Law Review of Kyiv University of Law*, 4, pp. 360-364.

[29] *Peck v. the United Kingdom* (2003) No. 44647/98., ECHR 2003-I.

[30] Rojszczak M. (2020) Does Global Scope Guarantee Effectiveness? Searching for a New Legal Standard for Privacy Protection in Cyberspace. *Information & Communications Technology Law*, 29 (1), pp. 22-44.

[31] *Roman Zakharov v. Russia* (2015). No. 47143/06, ECHR 2015.

[32] *Rotaru v. Romania* (2000) No. 28341/95, ECHR 2000-V.

[33] *S. and Marper v. the United Kingdom* (2008) nos. 30562/04 and 30566/04, ECHR 2008.

[34] *Satakunnan Markkinaporssi Oy and Satamedia Oy v. Finland* (2017). No. 931/13, ECHR.

[35] *Segerstedt-Wiberg and Others v. Sweden* (2000) No. 62332/00, ECHR 2006-VII.

[36] *Tyrer v. the United Kingdom* (1978) No. 5856/72, ECHR, Series A no. 26.

[37] Tzanou M. (2013) Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a not so New Right. *International Data Privacy Law,* 3(2), pp. 88-99.

[38] UN Human Rights Committee (HRC) (1988) *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April. Available from: https://www.refworld.org/docid/453883f922.html [Accessed 11 January 2021].

[39] *Uzun v. Germany* (2010) No. 35623/05, ECHR 2010.

[40] Van der Sloot B. (2014) Privacy as Human Flourishing: Could a Shift Towards Virtue Ethics Strengthen Privacy Protection in the Age of Big Data? *JIPITEC,* 5(3), pp. 230-244.

[41] Van der Sloot B. (2015) Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data". *Utrecht Journal of International and European Law,* 31(80), pp. 25–50.

[42] Van der Sloot B. (2020) The Quality of Law: How the European Court of Human Rights Gradually Became a European Constitutional Court for Privacy Cases. *JIPITEC,* 11(2), pp. 160-185.

[43] *Z v. Finland* (1997) No. 22009/93, ECHR, Reports of Judgments and Decisions 1997-I.

[44] *Zaichenko v. Ukraine (No.2)* (2015) No. 45797/09, ECHR.

DOI 10.5817/MUJLT2022-1-3

BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE: CONNECTING TWO DISTINCT TECHNOLOGIES TO COMPLY WITH GDPR'S DATA PROTECTION BY DESIGN PRINCIPLE

by

DÁNIEL ESZTERI*

The aim of the paper is to present some of the general principles of data protection law that can be applied to automated decision-making applications embedded into blockchain technology in order to comply with the provision of the European Union's General Data Protection Regulation (GDPR). The analysis focuses on the applicability of the 'data protection by design' principle during the development of such systems. Because blockchain-based networks are built on distributed data processing operations, therefore data controlling or processing of participating nodes should comply some abstract data protection patterns predetermined and collectively built-in during the system's development phase. On the other hand, the imprint of AI's automated data processing could be also observed and tracked back in the blockchain due to its historically retroactive nature. In the end, the study presents the human mind and its 'uploading' with conscious and unconscious contents as an analogy to blockchain-based AI systems. My goal is to highlight that the synergy of blockchain and machine learning-based AI can be hypothetically suitable to develop robust yet transparent automated decision-making systems. The compliance of these distributed AI systems with data protection law's principles is a key issue regarding the high risks posed by them to data subjects rights and freedoms.

* daniel.eszteri@outlook.com, Head of Data Breach Notification Unit at the Hungarian National Authority for Data Protection and Freedom of Information, lecturer in data protection law at Eötvös Loránd University Faculty of Law and National University of Public Service, Hungary.

KEY WORDS
General Data Protection Regulation, GDPR, Blockchain, Artificial intelligence, Machine learning, Automated decision making, Data protection by design

1. INTRODUCTION

Blockchain (a distributed data processing network technology) and artificial intelligence (AI) are two fields of technological developments that are being heavily discussed in legal scientific literature nowadays. As of now legal literature tends to examine these topics separate from each other.

However, these innovations can be applied jointly and will likely converge in the future. One possible connection between these technologies could be that blockchain provides the infrastructure for data processing and sets up the rules of engagement, while AI optimizes processes and rules. Data can be collected by IoT devices or just simply loaded into the system by the data controller as an already available training database.

In my paper I would like to identify and examine the connections of these apparently remote topics in order to strengthen the discussion on them in terms of the European Union's General Data Protection Regulation (GDPR). In the analysis I take it as a prerequisite that personal data should be processed in the blockchain and some kind of automated decision--making mechanism should be also present with the personal data without human intervention. With the creation of a system like this, the concept of blockchain-based AI can be made which can heavily affect the fundamental rights and freedoms of data subjects.

Blockchain-based data processing systems equipped with AI could pose a risk to the rights and freedoms of individuals because they could be built around two quite new and less mature technologies. In the first part of the study the nature of the two examined technologies will be presented from a data protection point of view, then in the second part, I shall attempt to present the problems stemming from the connection of the technologies.

2. NATURE OF DATA PROCESSING BASED ON BLOCKCHAIN TECHNOLOGY

2.1 BLOCKCHAIN AS A NETWORK FOR DATA PROCESSING

Blockchain-technology is a representative of the so called 'distributed ledger technologies', which was also frequently implemented into real practice

during the last decade, mostly in the form of cryptocurrency networks. Distributed ledger is a transactional database which is distributed on a network of more computers thus it is not stored in a central place. The term blockchain stems from the attribute of the system that transactions are stored in groups in the so-called blocks. The blocks form a chain connected to each other in chronological order.[1]

Blockchain can be described, in an intentionally simplified way, as a data storing and authenticating system. Prerequisite of this data storing and authenticating system is a distributed network consisting of computers with no subordination or superiority to each other. Computers connected to the distributed network function as 'nodes' which are also connected with each other. In the end, every node is connected somehow to all of the others. The advantage of this network is that disconnection of a node does not make any disruption in the system, because their tasks can be taken over by any other node.[2]

Data packages in the blockchain can be suitable to store any type of information so the technology can be used universally for nearly any kind of data processing purpose.[3]

2.2 THE BLOCK AS A UNIT FOR STORING DATA

In networks built on blockchain technology data is stored in the so-called blocks. According to some views, blocks can be seen as a blank paper, document or board to which any information can be written.[4]

Thus, we can treat a block in the moment of its creation as "tabula rasa" based on the concept of empiricist philosophy. With this concept, philosophers of the empiricist school wanted to convey that the human mind – as some kind of information processing medium – does not include any inborn, original knowledge at the moment of birth.[5] On the contrary,

---

1 European Central Bank. (2017) *How could new technology transform financial markets? 19th April 2017.* [online] Available from: www.ecb.europa.eu/explainers/tell-me-more/html/distributed_ledger_technology.en.html [Accessed 08 February 2021]

2 Győrfi, A. et. al. (2019) *Kriptopénz ABC (Cryptocurrency ABC).* Budapest: HVG Books, pp. 57-59.

3 For example blockchain can be used as a good tool for identity management purposes. In: Shraddha, K. (2018) Building-Blocks of a Data Protection Revolution – The Uneasy Case for Blockchain Technology to Secure Privacy and Identity, *Munich Intellectual Property Law Center - MIPLC Studies*, Vol. 35., 1. Edition 2018, Available from: doi.org/10.5771/9783845294025 [Accessed 11. November 2021], pp. 31-33.

4 Győrfi, A. et. al. (2019) op. cit., p. 60.

5 See e.g. Aristotle (in "On the Soul") and later in the Enlightenment John Locke ("An Essay Concerning Human Understanding"). In.: Andrássy, G. (2008) *Philosophy and Legal Ethics*. Dialog Campus, Pécs, pp. 32-33, 67.

representatives of the school of rationalist philosophy are on the standpoint that the mind of every human being includes some predetermined ideas or patterns that are present from the moment of birth in its deeper layers.[6]

Depending of the purpose of the given blockchain's creation, blocks as data storing units can store any kind of data and related information. Blocks storing information are connected to each other in a chain-like, posteriorly unchangeable way, which means that new blocks containing new data are always being connected to the end of the chain. The first created block in the beginning of the chain is called the 'genesis-block'.[7]

Regarding data processing, there is no actual data transfer between blocks in the blockchain network. This means that the execution of data processing operations with data stored in the blocks happens so that the network only assigns the 'right of disposal' to the given dataset. Technically speaking, the network assigns the 'digital signature' (via hashing) of users to the stored datasets and decides this way that who will have the right to disposal, access etc. on the given data.[8]

The network is built up like a chain and new data is added in newly created blocks which constitutes the ever-growing network of the blockchain. The log and hashes of every data processing operation is also stored in the individual blocks alongside the data itself (the summary of transactions results in the so called Merkle-tree).[9] The history of data processing operations is called the 'block-history'.

The algorithmic verification of every single data processing operation with the data stored in the blocks is the task of the computers (the nodes) connected to the network.[10]

During the approval of an operation, the following two elements will be verified by the nodes: Is the operation appropriately signed with the digital

---

[6] See for example Plato's thoughts on the world of ideas (in "Parmenides") at the earliest, and later, for example, Descartes takes a position in favour of rationalism against the concept of tabula rasa (in "Discourse on the Method"). In.: Andrássy, G. (2018) op. cit., pp. 35, 73.

[7] Győrfi, A. et.al. (2019) op. cit., p. 61.

[8] Hungarian National Authority for Data Protection and Freedom of Information. (2017) Opinion on Blockchain Technology in the Context of Data Protection (18th July 2017). Available from: *https://naih.hu/data-protection/decisions* [Accessed 08 February 2021], p. 3.

[9] Frankenfield, J. (2021) Merkle Root (Cryptocurrency). Available from: https://www.investopedia.com/terms/m/merkle-root-cryptocurrency.asp [Accessed 22 December 2021]

[10] Kakavand, H. et. al. (2017) The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849251 [Accessed 13 February 2021], pp. 4-7.

signature of the initiating party and does it have any authentic previous history on the blockchain.

If the nodes (or a predetermined number of them) approve the operation, than it is recorded in the block which will be stored in the chain in an unchangeable way. Further guarantee of credibility is that every single node will download a copy of the blockchain in order to continuously monitor each other for verification purposes and to share the newest copy of the database with each other.[11]

Based on the information above, we can describe blockchain in the simplest way as a data processing technology that enables processing of data on a joint, distributed network which is functional without the existence of any central verification body. The verification of data processing operations on the network is ensured by algorithmic based self--checking mechanisms.

3. ESSENTIAL CHARACTERISTICS OF MACHINE LEARNING TECHNOLOGIES AND THEIR CONNECTION WITH BLOCKCHAIN

3.1 GENERAL TECHNOLOGICAL BACKGROUND OF MACHINE LEARNING

I would like to highlight and present the technological background of AI and machine learning only to the extent, that is necessary to understand and analyse the model of blockchain-based AI and ML from a legal point of view.

The report of the Norwegian Data Protection Authority (Datatilsynet) describes AI as a system capable of learning based on its own experience and to apply the knowledge obtained in different situations to resolve complex problems. The heart of the concept is that AI learns from the personal data it 'sees' (in practice the input data) and makes decisions or 'forecasts'.[12]

AI on the other hand serves as an umbrella term, which covers all the procedures when a software makes a decision automatically.[13] Relative

[11] Győrfi, A. et.al. (2019) op. cit., pp. 63, 68.

[12] Datatilsynet. (2018) Artificial intelligence and privacy. Available from: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf [Accessed 8 February 2021].

[13] Commission nationale de l'informatique et des libertés (CNIL) (2017). How can humans keep the upper hand? The ethical matters raised by algorithms and artificial intelligence. Available from: https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_

to this, machine learning (ML) is a narrower concept, which means one branch of AI development. The heart of this is that the system generates independent knowledge out of its own experience.[14] Based on data examples and patterns, the system is able to recognise and determine regularities and rules independently or with human assistance and then makes decisions based on the regularities discovered in the acquired knowledge base.[15]

Data processing carried out by an AI system in the course of ML can be divided into three steps as follows:

(1) First, a large quantity of data is input in the system and the algorithm tries to find patterns and similarities in this data set. If the algorithm finds identifiable patterns, it will record and save them for subsequent use. After this, the system generates a model on the basis of the recorded and saved patterns. Based on the already identified patterns, with the help of the model, the system is capable of processing the subsequently input data.

(2) After this, the AI system operates as follows: first, new data are uploaded in the system, which are similar to the data used for learning. Then, based on the model, the AI decides which new data are similar to which learned pattern.

(3) Finally, the system makes a decision based on the acquired patterns with the new input data and informs the observer about the decision.[16]

It is also important to note that the model generated in the course of machine learning does not necessarily contain the source data, which served as the basis of its learning. In most cases, the AI system generated in the course of ML is able to operate independently of the data that served as the basis of learning.[17]

---

gb_web.pdf [Accessed 23 July 2021], pp. 16-17.

[14] Szepesvári, C. (2005) Machine learning – a brief introduction. [lecture] MTA SZTAKI. Available from: http://old.sztaki.hu/~szcsaba/talks/lecture1.pdf [Accessed 9 February 2021].

[15] European Union Agency for Fundamental Rights. (2019) Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights. Available from: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf [Accessed 22 July 2021], pp. 4-5.

[16] Datatilsynet. (2018) op. cit., p. 7. and European Union Agency for Fundamental Rights (2019) op. Cit., pp. 4-5.

[17] Datatilsynet. (2018) op. cit., p. 10.

Characteristically, ML requires a much larger quantity of raw data than the human brain does in order to be able to efficiently identify patterns and to set up decision-making models on their basis. So, at first, we might think that the more data we have, the better AI systems based on machine learning we can produce. Yet, the quality of the data used for machine learning, their appropriate prior selection and labelling are much more important aspects. Even before inputting the data in the system, it is necessary to clarify the exact purpose of using the data to carry out specific tasks and because of this, the range of the data used must be restricted to those relevant for the given purpose. The good selection and preliminary choice of the data used is also a very important criterion.[18]

3.2 AUTOMATED DATA PROCESSING ON THE BLOCKCHAIN NO 1.: SMART CONTRACTS

Researchers dealing with distributed ledger systems already described the possibility of automatization of data processing operations in the blockchain by running algorithms on the network.

It was Nick Szabo who described for the first time – using the concept and term of "smart contract" in 1996 –, the automatization of data processing operations in a distributed network. According to Szabo, a smart contract is such a contract that is being automatically fulfilled if its previously specified conditions are met, therefore the contract is unbreachable. When the contractual conditions are met, than the fulfilment, security and inviolability of the contractual terms are being secured by the computer network in which the parties created it. Therefore, the contracting parties do not need to rely on the assistance of a third party, for example a lawyer, for authentication.[19]

As it can be already seen in practice, blockchain is a fully viable technology for running smart contract applications: the possibility for users to enter into smart contracts was introduced by the blockchain-technology--based platform, Ethereum.[20] In essence, the program running on the network automatically executes a certain decision when the required conditions are met.

In the case of smart contracts, the verification of the operations and

[18] Datatilsynet. (2018) op. cit., p. 11. and European Union Agency for Fundamental Rights (2019) op. cit., pp. 10-12.

[19] Szabo, N. (1996) Smart Contracts: Building Blocks for Digital Markets. Available from: www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf [Accessed 8 February 2021], pp. 1-5, 8.

[20] Buterin, V. (2013) A Next-Generation Smart Contract and Decentralized Application Platform. Available from: https://ethereum.org/en/whitepaper [Accessed 14 February 2021].

the processed data is the task of the network nodes. Verified data can be, for example, the bank account number of contracting parties, the amount, relevant dates (e.g. deadlines), other terms, related personal data (e.g. names), and even other textual information (e.g. statement, short message) could be recorded. Therefore, a smart contract embedded in blockchain is dependent on outside input. Data, executed operations and other information relevant in the context of the contractual conditions are recorded and logged in the blockchain in an unchangeable way.[21] According to a more technical perspective, for example, the hash of a file and the owner's name can be stored as pairs in the code to achieve the functionality of proof of ownership. The hash of a file and the block's timestamp can also be stored as pairs to realize the proof of existence function.[22]

The smart contract application runs on every node of the distributed network, so every user can benefit of it and use its functions. The code and algorithm of the smart contract application responsible for automatization is available, accessible and usable by every participant of the network.[23]

However, smart contract applications should not be mistaken with AI techniques. Smart contract applications cannot be treated as AI applications on their own, because they do not make individual decisions based on data in the blockchain. The main purpose of smart contracts in most situations is only to automatize and authenticate transactions on the blockchain when certain conditions met. In most cases do not feature a great deal of complexity.[24] Based on the above, AI and ML can enhance the efficiency of smart contracting applications but smart contracts are not considered AI themselves.

3.3 AUTOMATED DATA PROCESSING ON THE BLOCKCHAIN NO. 2.: A DISTRIBUTED AI?

Turning back to the blockchain as the starting point of our topic: if we would run an analyser software on the blockchain which is capable

---

[21] Filatova, N. (2020) Smart contracts from the contract law perspective: outlining new regulative strategies, *International Journal of Law and Information Technology*, Volume 28, Issue 3, Autumn 2020. Available from: https://doi.org/10.1093/ijlit/eaaa015 [Accessed 14 February 2021], pp. 220-222.

[22] Xing, B. and Marwala, T. (2018) The Synergy of Blockchain and Artificial Intelligence. Available from: http://dx.doi.org/10.2139/ssrn.3225357 [Accessed 23 July 2021], p. 3.

[23] Bacon, J. et. al. (2017) Blockchain Demystified. *Queen Mary School of Law Legal Studies Research Paper* No. 268/2017, p. 29.

[24] Schrepel, T. (2021) Smart Contracts and the Digital Single Market Through the Lens of "Law + Technology" Approach. European Commission. Available from: https://ssrn.com/abstract=3947174 [Accessed 26 December 2021].

to identify patterns in the stored data by ML techniques, than it could become suitable to also make decisions automatically.

I emphasize – as it was already covered in literature – that blockchain-based data processing can be assisted or enhanced via various AI techniques.[25]

In my opinion there are two possibilities to run AI applications on the blockchain:

(1) *The blockchain-based machine learning approach:* AI analyzes data processing operations in blockchain and tries to identify patterns. In this case blockchain means the storing form and source of the training data. The identified patterns constitute a model which can later be used to produce a decision based on the identified patterns and also to increase system efficiency. In this case, blockchain stored data should serve as and input for AI-based data processing.

(2) *The blockchain-based automated decision making approach:* AI executes data processing operations on the blockchain and tries to optimize decisions at the same time. In this approach decisions made by the AI algorithm should also be logged in the blockchain itself (in fact: in the block-history and Merkle tree), as it was indicated in chapter 2.2. of the paper. In my opinion, it could be also possible to store a copy of the logs of the decisions in a separate (not necessarily blockchain-based) database as well, but it is not fundamentally necessary for the working mechanisms of such systems.

A collection of projects on applications or software capable of making automated decisions with processed data in the blockchain can be found in recent research papers in the field.[26] Moreover, a collection of blockchain-based AI projects can be found in recent paper of Vasco Lopes and Luís A. Alexandre (for example using blockchain to store "robotic events").[27] According to them, blockchain-based automated decision making

[25] Xing, B. and Marwala, T. (2018) op. cit., pp. 6-8.

[26] See, for example, the following study on the concept of blockchain-based profiling for energy management purposes: Sankaran, S. et. al. (2018) Towards Realistic Energy Profiling of Blockchains for Securing Internet of Things. *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)* Vienna.

[27] Lopes, V. and Alexandre, L. A. (2019) An Overview of Blockchain Integration with Robotics and Artificial Intelligence. *Ledger Journal Vol. 4, Supplement 1 (2019): Proceedings of the First Symposium on Blockchain and Robotics,* MIT Media Lab, Cambridge, MA, 5 December 2018, USA. Available from: https://doi.org/10.5195/ledger.2019.171 [Accessed 23 July 2021].

applications search patterns in the database and make decisions based on the identified model.

In this paper I consider as a prerequisite that purely automated (algorithm-based) decisions are made with personal data stored in the blockchain without any human intervention.

3.4 EXAMPLES ABOUT THE SYNERGY OF BLOCKCHAIN AND AI

A good model can be found in the paper of Sandner et. al. about the synergy of blockchain and AI: in the hypothetic example a network of street lamps in a smart city constitutes the blockchain and every lamp has its own identity (block) on the network. Since all lamps are connected to a blockchain they will store data about their usage, performance and downtime. AI could analyse this data and optimize the network's maintenance. For example suggests a more regular maintenance of more frequently used lamps etc.[28]

We can apply this example to a more personal data processing based system: for example, in Article 29 Working Party's (WP29) opinion, smart grids and smart metering has been already analysed from a data protection point of view.[29] The antecedent of the opinion was the European Commission's recommendation on preparations for the roll-out of smart metering systems. In the context of the recommendation smart grid means "an upgraded energy network to which two-way digital communication between the supplier and consumer, smart metering and monitoring and control systems have been added." Furthermore smart metering means "an electronic system that can measure energy consumption, adding more information than a conventional meter, and can transmit and receive data using a form of electronic communication."[30] Smart meters can actually be considered as a digital version of conventional meters, except that smart

[28] Sandner P. et. al. (2020) Convergence of Blockchain, IoT, and AI, Front. *Blockchain 3:522600.* Available from: https://doi.org/10.3389/fbloc.2020.522600 [Accessed 11. November 2021.], p. 4.

[29] Article 29 Data Protection Working Party. (2013) Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force (WP209). Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf [Accessed: 25 November 2021].

[30] European Commission. (2012) Recommendation on preparations for the roll-out of smart metering systems (2012/148/EU) 9 March 2012. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012H0148& [Accessed: 15 December 2021], Article 1(3), (a)-(b).

meters act as a two-way communication channel between consumers and service providers (e.g. electricity, water, gas). The advantage of smart meters is that they transmit detailed and real-time consumption information to the provider in a simple and direct way. Consumers will receive a very detailed statement of their energy consumption based on real-time quantitative data, which will make their consumption easily optimisable.

The recommendation and the opinion already drew high attention to the requirements and enforcement of the principles of 'data protection by design and default' in the context of the planning and operation because huge amount of personal data about the consumers will be processed in such systems.[31]

If we apply the above mentioned hypothetic example of Sandner et. al. (blockchain-based street lamps) to a smart grid and smart metering system, we can say that individual households could constitute the blocks of the network. They can store data about their consumption of water, gas, electricity etc. and send it real time to the service providers. On the other hand AI and ML technologies could also analyse the consumption data of households and identify 'consumption-patterns' in order to optimize energy distribution between customers. Individual service providers could also share the identified data-processing patterns with each other to synchronize their services for a better service distribution.

In such systems, the history of consumption data will be recorded in the blocks (households) as well and can be tracked back historically. The effectiveness of consumption optimization by ML can also be followed in the blocks by tracking back consumption details of individual households. This could also make the system more transparent and help to develop further the applied AI and ML techniques for a better functioning smart grid and smart metering system.

The recent report prepared for the European Commission and the European Investment Bank also took note that in the energy sector the synergy of these technologies can be used: AI to optimise energy use in the buildings and blockchain to share data to across the energy industry to optimise network usage.[32]

---

[31] European Commission (2012) op. cit., Article 1(3), (d)-(e).

[32] Verbeek A. and Lundquist M. (2021) Artificial intelligence, blockchain and the future of Europe: How disruptive technologies create opportunities for a green and digital economy. Available from: https://op.europa.eu/en/publication-detail/-/publication/8730fef5-315c-11ec-bd8e-01aa75ed71a1/language-en [Accessed 21 December 2021], p. 109.

4. DATA PROTECTION ISSUES OF THE BLOCKCHAIN – AI SYNERGY

4.1 RULES ON AUTOMATED DECISION-MAKING IN THE GDPR

The GDPR, does not define the concept of *automated decision-making*, however it uses this expression several times in the normative text. On the other hand, the concept of *profiling* is included in the list of definitions of Article 4.

According to this provision, profiling means any form of automated processing of personal data to evaluate certain personal aspects of a natural person. In particular to analyse or predict the natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.[33]

According to the relevant guidance of Article 29 Data Protection Working Party (WP29), automated decision-making is a capability of making decisions with the help of technological instruments without human intervention.[34] That is to say, there is no human involvement in decision-making in the case of exclusively automated decision-making.

Pursuant to Article 22(1) of GDPR, the data subject shall have the right not to be *subject to a decision* based *solely on* automated processing, *including profiling*, which produces *legal effects concerning him or her or has similarly significantly impact on him or her*. This provision constitutes a general prohibition on decision-making based exclusively on automated data processing. The regulation includes profiling based on such a decision--making process. This prohibition stands irrespective of whether or not the data subject takes any measure concerning the processing of his/her personal data. Therefore, as a main rule GDPR sets forth a general prohibition on exclusively automated individual decision-making, which produces legal effects or similarly significant impact.[35]

In order to qualify an activity as human intervention with regard to the decision and therefore the general prohibition of Article 22 should not apply to it; the controller has to ensure that the human review of the decision be of merit and not only a symbolic gesture. It has to be done

---

[33] GDPR Article 4(4).

[34] Article 29 Data Protection Working Party. (2017) op. cit., p. 8.

[35] Veale, M. and Edwards, L. (2018) Clarity, surprises and further questions in the Article 29 Working Party draft guidance on automated decision making and profiling. *Computer, Law and Security Review 34(2),* p. 400.

by a person, who has the authority and the competence to alter the decision. In other words, to be exempt from the prohibition, the final decision must be made by a human, or the decision proposed by the algorithm has to be reviewed and approved by them.[36]

Furthermore, the rules applicable to exclusively automated decision--making have to be applied only in the cases when the decision has legal effects or similar significant impact on the natural person. GDPR does not define the notions of "legal effect" or "similarly significant", but this wording of the regulation makes it clear that Article 22 extends only to effects involving severe consequence.[37]

The legal effect requires that the decision should influence the legal rights of a person. A legal effect may be something that will influence the legal standing of a person or his/her rights based on contract. According to WP29, examples of such effects include automated decisions concerning natural persons as a result of which: contracts are terminated, welfare benefits (such as child-related benefits or housing support) guaranteed by law are granted or rejected, entry to a country is refused, citizenship is denied etc.[38]

The effect of automated decision-making on the rights of people set forth in law or contract concerns cases that can be relatively clearly delineated. In addition, however, there is the more vaguely worded "similarly significant" impact in Article 22, which is also a circumstance subject to the prohibition. Recital (71) of GDPR may contain some guidance concerning this notion as it lists the following examples: "refusal of an online credit application" or "e-recruiting practices without any human intervention".

There are, however, exemptions from this general prohibition set forth in Article 22(2). Accordingly, the prohibition cannot be applied, if the decision is:

(1) necessary for entering into or performing a contract between the data subject and the data controller;

(2) authorised by European Union or Member State law, *to* which the data controller is subject and which also lays down suitable

[36] Article 29 Data Protection Working Party. (2017) Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251rev.01). Available from: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 [Accessed: 8 February 2021], p. 22.

[37] Veale, M. and Edwards, L. (2018) op. cit., p. 401.

[38] Article 29 Data Protection Working Party (2017) op. cit., p. 22.

measures to safeguard the data subject' rights and freedoms and legitimate interests; or

(3) based on the data subject's explicit consent: A clearest method of gaining assurance that the consent was expressed is a written statement of the data subject. According to the European Data Protection Board, in a digital or online context it may happen for instance that the data subject can issue the required statement by completing an electronic form, sending an e-mail or uploading a scanned document containing his signature or using an electronic signature. Finally, one can gain assurance of the validity of the express consent through the two-step control of the consent (a good example of this is the use of two stage verification).[39]

4.2 BLOCKCHAIN-BASED AUTOMATED DECISION MAKING AND THE GDPR

Therefore, where personal data is processed in the blockchain for automatic decision-making purposes, the controller must comply with the above requirements of the GDPR as well. Of course, it will always be the data processed, the specific purpose of the processing and its impact on the data subject that determines whether the rules of Article 22 applies or not. If so, data processing using automated decision-making is only possible on the blockchain if the controller can demonstrate the legitimate use of the exceptions above.

The common feature of applications running on blockchain that are capable of automated decision-making (including profiling in particular cases) should be that their decisions are based on the data processed in the distributed network and are free of any human intervention. In these cases Article 22 of the GDPR applies to such systems.

If we take the hypothetic example of blockchain-based smart metering from point 3.4. of the paper, in my opinion, such data processing falls under the ruling of Article 22, because automatic decisions influence the legal rights of persons (e.g. the right for electricity supply) and the processing is based on a contract between the data subject (customer) and the data controller (e.g. electricity service provider).

[39] European Data Protection Board. (2020) Guidelines on consent under Regulation (EU) 2016/679. Available from: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf [Accessed 30 December 2020], pp. 20-22.

4.3 COMPLIANCE WITH THE PRINCIPLES OF PURPOSE LIMITATION AND DATA MINIMIZATION

Blockchain-based data processing can cause serious confusion about its possible compliance with the GDPR's principles of purpose limitation and data minimization. On the basis of the purpose limitation principle, personal data should only be collected for a specific, clear and legitimate purpose and should not be processed further in a manner that is incompatible with those purposes.[40] According to the principle of data minimization, the personal data processed should be adequate and relevant for the purposes of processing and limited to what is necessary in relation to that purposes.[41] Both principles constitute a prohibition on the processing of exaggerated, stockpiling, unnecessarily handled and stored data.

One of the basic principles of blockchain is that all the data is stored in the database even after transactions or other operations with them are performed. Newer data processing operations will be connected via hashing to older ones to ensure integrity and security. More simply: data and transaction logs are supposed to be stored indefinitely in the system, so that one can accurately trace back individual data processing operations. The 'replicative' nature of the blockchain is also problematic from a data protection point of view when all nodes store a complete copy of the database for self-checking purposes.[42] At first sight, these characteristics are in contrast to the principles of the GDPR referred above.

However, it is a very important preliminary question for assessing the legality of blockchain-based data processing, that to what level the processing is compatible with the original purpose.[43]

Blockchain-based data processing can only comply with the principles of purpose limitation and data minimization if such type of processing of personal data (e.g. storing data in the chain) is compatible with the original purpose. There are types of data processing that are fundamentally not suitable for this. For example, data processing based on the consent of the data subject is almost never, since (at first sight), it is

[40] GDPR Article 5(1)(b).

[41] GDPR Article 5(1)(c).

[42] Finck, M. (2019) Blockchain and the General Data Protection Regulation. European Parliamentary Research Service, PE 634.445, p. 68.

[43] Finck, M. (2019) op. cit., p. 65.

impossible to carry out the obligation to delete personal data if the consent is withdrawn.[44]

However, in the case of data processing based on compliance with a legal obligation, such as the keeping of real estate registers[45, 46] or state archives, the situation is easier, since the purpose of these databases is to preserve and to keep accurate all personal data and all of the operations carried out with them.

Therefore, it is necessary to declare that a given blockchain-based data processing can only be assessed on a case-by-case basis from the perspective of legality and GDPR-compliance. Having regard to purpose limitation and data minimization, special attention should be paid to the selection of the appropriate legal basis for data processing. If the predetermined legitimate purpose of processing can comply with the specificities of blockchain technology, compliance with the principle of data minimization will not be problematic any longer.

If the controller wishes to use automatic decision-making algorithms for blockchain-based processing, of course, this processing operation must also be examined for compliance with the abovementioned principles.

In my opinion, if the purpose of data processing is legally compatible with the characteristics of the used technology, the operation of the automatic decision-making application using the data processed will be also compatible with it in most cases. The reason for this is that the data is stored in the blockchain itself, and automatic decision-making is only being 'built on' the database. Nevertheless, it is also important to examine the compliance of the system with the specific rules of the GDPR on automatic decision-making (see point 4.1. of this paper).

However, I stress that before loading data into the system, it is necessary to clarify exactly what kind of task the data is used for and therefore limit

---

[44] GDPR Article 17(1)(b): The data subject shall have the right to delete the personal data relating to him or her without undue delay at his request and the controller shall be obliged to delete the personal data relating to the data subject without undue delay if [...] the data subject withdraws the consent of the data subject on the basis of Article 6(1)(a) or Article 9(2)(a) and there is no other legal basis for processing.

[45] McMurren, J. et. al. (2018) Adressing Transaction Costs Through Blockchain and Identity in Swedish Land Transfers. Available from: blockchan.ge/blockchange-land-registry.pdf [Accessed 13 February 2021].

[46] Kachorowska, M. (2019) Blockchain-based land registration: Possibilities and challenges. *Masaryk University Journal of Law and Technology, Vol. 13. No. 2*. Available from: https://doi.org/10.5817/MUJLT2019-2-8 [Accessed 13 February 2021].

the range of data used to those relevant to the purpose.[47] This is also a key requirement for the application of the principle of data protection by design, which will be described later.

4.4 COMPLIANCE WITH THE PRINCIPLE OF TRANSPARENT DATA PROCESSING

One of the most frequently expressed concerns in relation to machine learning (and not only from the viewpoint of data protection) is that it is often impossible to predict what sort of result the system will produce. The model applied may produce a result, for which seemingly no explanation exists.[48] This phenomenon is referred to in machine learning as "black box". For an ordinary observer, the system works in practice by absorbing data on the input side, on the basis of which it learns something, then it produces some result. It is, however, extremely difficult to see why exactly it generated that result.[49]

The size of the network and the connections between the individual layers may render data processing tasks so complex that cannot be understood by humans, even data scientists. They just do not know what happens in the black box.

In scientific and technical fields, the black box is a device, system or object, which can only be examined on the basis of its input, output and transmission characteristics, its concrete internal operation is unknown, that is, its implementation is 'opaque' (black).[50]

Because of this, undertakings developing data processing based on AI solutions may be seriously challenged by the legal requirement of transparency in that regard.

The requirement that data processing must be transparent for the data subject (whose data are being processed) has been included among the principles of data protection for a long time. This principle is expressly named in the GDPR in Article 5(1)(a). Accordingly, personal data shall be

---

[47] Datatilsynet. (2018) op. cit. p. 11. and European Union Agency for Fundamental Rights (2019) op. cit., p. 10.

[48] Datatilsynet. (2018) op. cit., p. 12.

[49] Infostart. (2018) *Belenéztek a fekete dobozba az ELTE kutatói (Researchers of Eötvös Lóránd University looked into the black box)* [press release] Available from: https://infostart.hu/tudomany/2018/11/16/melytanulasi-halozatot-vizsgaltak-az-elte-kutatoi [Accessed 13 February 2021].

[50] Cauer, E. et. al. (2000) Life and Work of Wilhelm Cauer (1900–1945). *Proceedings of the Fourteenth International Symposium of Mathematical Theory of Networks and Systems (MTNS2000)*, p. 4.

processed lawfully, fairly and in a transparent manner in relation to the data subject. That is to say GDPR names the principles of lawfulness, fairness and transparency at the same time, hence they must be enforced in relation to every data processing operation with respect to one another and simultaneously.

A question therefore is how systems using machine learning can be set up so that they operate with sufficient transparency for the data subject from the viewpoint of the results they produce. The primary issue in relation to these data processing methods is whether it complies with the principle of transparency.

GDPR requires the controller to provide information in relation to decision-making based exclusively on automated data processing having legal effects or similarly significant effect. The regulation here also includes profiling based on such data processing.[51] Under this, the following three items of information must be communicated with the data subject:

(1) He must be informed of the fact of such data processing;
(2) He must be given information of merit on the logic applied; and
(3) Finally, he must be informed of the significance of the data processing and its expected consequences for the data subject.[52]

According to GDPR, controllers must provide "information of merit" on the logic applied. If a controller communicates only in general that it is, for example, "operating a system based on a neural network" may not be sufficient, as the data subject will have little idea of what is happening with his personal data in the course of processing.

The information of merit, however, does not necessarily mean that the controller should provide complicated explanations about the algorithm applied or present the algorithm in full. A detailed presentation of the technology would, in most cases, decrease the comprehensibility of the information and impede its reception.[53]

In addition to the above, it is necessary to note that the controller has to inform the data subject also about the "significance" and "expected consequences" of data processing. According to the WP29 guidelines, in order that this information be of merit and comprehensible, real and

[51] GDPR Article 15(1)(h).
[52] GDPR Article 13(2)(f).
[53] Attila Péterfalvi et. al. (2018) *Magyarázat a GDPR-ról (Interpretation of the GDPR)*. Budapest: Wolters Kluwer, p. 158.

tangible examples of possible effects should be given. In a digital context, controllers may also use additional instruments to present such effects and may apply visual techniques to explain a former decision. In such a case, the guidance gives the example of providing a comparable application.[54]

According to the joint research by the Oxford Internet Institute and the Alan Turing Institute of London, it may be also a good practice from the viewpoint of the transparency of the decisions made by the algorithms and the related data processing, when the controller provides an opportunity for the data subject to learn the operation of data processing by making available a test system for them.[55] In this way, the controller does not need to 'open the black box' to the data subject. It is sufficient, if it makes the data subject understand how the decision was made and what he can do in order to have a different (more favourable) decision in his case.[56]

In order to comply with the obligation of transparent data processing, the operation of a blockchain-based system may even be desirable. This is because all data processing operations in the blockchain are logged and stored in the database and are accessible to all nodes in the block-history. Of course, the log of operations stored in the blockchain contains only the results of the decisions, and not necessarily how the decision itself was made by the automatic decision-making software. However, all actions with the data can be studied by the users, which can make it easier to deduce or understand the logic behind the decision made by the algorithm.

5. APPLYING DATA PROTECTION BY DESIGN TO BLOCKCHAIN-BASED AUTOMATED DECISION--MAKING

5.1 IMPRINT OF DATA PROCESSING OPERATIONS IN THE BLOCKCHAIN

The GDPR mentions, among the general obligations of the controller and the processor, that they should incorporate various guarantees into the process in order to comply with data protection principles and the requirements of the regulation, as well as the rights of data subjects. These guarantees should cover appropriate technical and organizational

[54] Article 29 Data Protection Working Party. (2017) op. cit., p. 28.

[55] Wachter, S. et. al. (2018) Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR. *Harvard Journal of Law & Technology, 31 (2)*, pp. 863-871.

[56] Datatilsynet. (2018) op. cit., pp. 21-22.

measures that take into account the state of the art and the costs of implementation, the nature, scope, circumstances and objectives of the processing and the risks to the rights and freedoms of natural persons of varying likelihood and severity.[57] The controller shall implement appropriate technical and organizational measures to ensure that, by default, only personal data which are necessary for the specific purpose of processing are processed. This obligation applies to the amount of personal data collected, the extent to which they are processed, the duration of their storage and their availability. In particular, these measures should ensure that personal data are not accessible by default to an unspecified number of persons without the intervention of the natural person.[58] These provisions of the GDPR are called the principle of data protection by design and by default, whose function is to take compliance with the regulation by default at both the technical and organizational level when designing systems for data processing.

Compliance with this principle is also necessary for blockchain-based personal data processing and automated decision-making applications based on it, so developers should always take a close look at the up-to-date techniques and organizational solutions available on the market and applicable to the technologies used.

This means that during the development and testing process of blockchain-based automated decision-making systems data protection compliance should be monitored and applied long before the start of live data processing. In this way data protection compliance would appear also when the live system begins to work in practice.

The following theory could be set up to follow the aforementioned principle: The block, as a data storage unit, may contain any (digitizable) personal data or information at the time it is added to the chain. The nature of the data and information processed can only be limited by the specific purpose. However, the operational principles of blockchain-based data processing will begin to be developed already before live personal data is added to the system. It is the responsibility of the controller and the processor to consider data protection compliance even in the early stage of development of the system, on the basis of the principle of data protection by design as described above. In doing so, it is necessary

[57] GDPR Article 25(1).
[58] GDPR Article 25(2).

to examine, inter alia, the requirement of purpose and storage limitation, or transparency as set out above, as well as the form of information provided to the data subject and the existence of a legal basis for automated decision-making. These are, of course, only steps on the path of GDPR--compliance because the controller should also consider compliance with the additional requirements of the regulation.

This is also important because the immutable storage of data and logging all of the data processing operations in the blockchain can serve as a kind of perpetual imprint for checking compliance (see for more details on processing point 2.1. and 2.2. of the paper). The indelible imprint of data processing operations in the blocks represents such processing patterns in which compliance with data protection law can be also examined. These patterns are available in all node-managed replicas of the blockchain. In my opinion, the imprint of these patterns can be also studied if the personal data are otherwise processed in a separate database using so-called off--chain solutions.[59]

5.2 IMPRINT OF AI'S OPERATION IN THE BLOCKCHAIN?

If automatic decision-making applications and algorithms are used in the blockchain-based system when processing personal data, the data processing operations carried out by such applications can be followed in the system's log (block history and Merkle tree). In my opinion the imprint of AI-made decisions with personal data can be followed and tracked back when AI executes data processing operations on the blockchain and tries to optimize decisions at the same time as it was indicated in point 3.3 of the paper ('blockchain-based automated decision--making approach'). In this approach decisions made by the AI algorithm should also be logged in the blockchain itself.

By examining the imprint, we could see the big picture of the decisions the algorithm is making with the data. By examining the patterns that each decision assembles, we could better understand the background of automatic decision-making and how the AI works. This may also be crucial for understanding the processes in the black box, which may ultimately facilitate information on the logic used in automated decision-

[59] Off-chain data processing is a blockchain-based technology in which personal data is stored in a separate database rather than in the blockchain itself, but is processed using hash keys to connect to the back-end core database, which is already blockchain-based. See: Mannan, R. et. al. (2019) GDPR and Blockchain: A Compliance Approach. *European Data Protection Law Review 2019(3)*, pp. 423-424.

-making and its importance and expected consequences for the individual, as set out in Article 13(2)(f) and Article 22 of the GDPR.

The design of the behavior of the blockchain-based distributed AI will be recorded in the blocks and will be collectively present in the data processing operations performed by all nodes. The main source about the imprint of the AI's operation could be the block-history.

I am of course aware, that the above theory is highly hypothetical for now, although I think that it could have some scientific and practical merit when designing or observing the work of such systems. In this way different large data controllers can process personal data in an automated way based on the same patterns and principles that blockchain solutions offer.

5.3 AN ANALOGY: COMMON FEATURES OF HUMAN CONSCIOUSNESS AND BLOCKCHAIN-BASED AI

Collective patterns of the functioning of human consciousness have previously been identified within the science of psychology, so I would like to introduce this before applying it to the AI and blockchain synergy. Among the representatives of the psychoanalytic school, Carl Gustav Jung pointed out in human history the identity and repetition of certain archetypic images and metaphors in each culture, which he describes as part of the "collective unconscious" of humanity. These collective psychic patterns are reflected in an individual's thought and behavior as well. Jung writes so of the collective unconscious:

> *"The collective unconscious is a part of the psyche, which owes its existence not only to personal experience, that is, we have not acquired it personally. The collective unconscious content was never conscious and therefore never acquired by the individual, but was fully inherited. While the personal unconscious consists of complexes, the collective unconscious contains archetypes. The concept of archetype expresses that there are certain forms in the psyche that can be found at all times and everywhere. The collective unconscious, like a second psychic system, is universal and impersonal in nature and is the same in everyone."*[60]

[60] Jung, C. G. (2017) *The collected works of C.G. Jung, Part 9/I.: The archetypes and the collective unconscious.* Budapest: Scolar, pp. 51-52.

In terms of classification into the philosophical schools of empirism and rationalism mentioned at the beginning of the paper (see point 2.2.), these ideas are more close to rationalism, according to which human consciousness has inherited patterns of thought and behavior.

Turning our view from the human consciousness and the collective unconscious of humanity to the examination of AI, according to Pokol, AI is becoming more and more entwined in humanity's mental layer today. The best example of this is that we are living in a society where communication is primarily based on networks of human-added and dynamically changing data flows. This phenomenon has changed the medium of communication from a physically fixed form (e.g. paper) to a state of "constant reflexive levitation" of human consciousness.[61] Kelly calls this "flowing", the fluidity of knowledge, or the phenomenon of "liquid shared intelligence" in humanity's new data-driven society.[62] The nature of communication using social media is a good example for this.

On the basis of the above, anyone in a data-driven society can add their knowledge and information to humanity's collective repository, which is an imprint of humanity's collective thinking and intelligence. AI algorithms can look for the correlations in this collective imprint of our mind and can show us similar patterns in the functioning of humanity's thinking and consciousness, including even unconscious content.

If blockchain-based data processing is compared to the human mind, we can say that individual blocks storing specific personal data may represent information stored by one's personal consciousness.

As explained above in points 5.1. and 5.2., the application of preliminary set data processing patterns in the blockchain can serve as a compliance tool to comply the data protection by design principle. Hypothetically, even the imprint of AI could be studied if automatic decisions making tools are also embedded in the blockchain.

The block in the blockchain, as a data storage unit, is thus in itself a 'tabula rasa' – using the term borrowed from empirical philosophical school –, at the moment of its birth, but the actual processing can only be carried out on the basis of data processing patterns designed by the data

[61] Pokol, B. (2018) Artificial Intelligence: The Emergence of a New Layer of Being? (AI in the Mirror of Nicolai Hartmann's Ontology). Available from: http://dx.doi.org/10.2139/ssrn.3225111 [Accessed 13 February 2021], pp. 1-2.

[62] Pokol, B. (2018) A *mesterséges intelligencia társadalma (Society of Artificial Intelligence).* Budapest: Kairosz, pp. 111-114.

controller. This is what makes these predetermined data processing patters a bit similar to collective unconscious of mankind.

In principle, the abstract rules and patterns that guarantee data protection compliance should be present when the first block is created with live personal data. Therefore, when the blockchain is being built, these patterns of legal compliance can "spread across" all blocks and all replicas of the blockchain managed by nodes. Later, the imprint of the operation of AI can be studied in the block-history. This feature could help to fine tune later data protection compliance as well.

6. SUMMARY: SYNERGY OF BLOCKCHAIN AND AI AS THE NEXT BIG PRIVACY CHALLENGE?

> *"It turned out that creating a god, as your forebears can attest, is not easy. Above all, we needed data. And he was our guy. Dempsey was rich, arrogant. He was in the right place at the right time, before the privacy laws. And his company, Incite, had all the data in the world."*[63]

We have seen above that it is possible to develop decision-making systems that can make decisions quickly and efficiently using patterns learned from personal data. Moreover, we also saw that blockchain is a data processing system that uses a distributed network structure to ensure a high level of data security and manage distributed resources efficiently. If a machine learning system uses personal data processed in a blockchain database to make decisions, it is a mix of the two systems.

According to some opinions, at first sight the development of AI and the basic operating principles of blockchain seem contradictory. This is because the efficient development of AI requires a large amount of up-to--date, high-quality data to properly teach algorithms and thus make accurate decisions.[64] As a result, only those data controllers will benefit who have the highest quality (up-to-date, accurate) data and state-of-the-art technology in their hands. Effective development today is therefore done by collecting large amount of high quality data and acquiring massive computing capability, and then focusing and centralizing it in one hand. Blockchain, on the other hand, is a technology based on the allocation of resources and data by eliminating central control, where data can be

[63] Westworld, Season 3, Episode 5.

[64] European Union Agency for Fundamental Rights (2019) op. cit., pp. 10-12.

accessed by all actors in the network.[65] However, the mixing of these controversial technologies can also lead to the democratization of the AI industry and a fair distribution of resources and data among smaller and larger players.[66] It could be also concluded that the decentralized nature of such systems may even make capable independent organizations to lawfully process data by the same data processing patterns in accordance with the GDPR's principle of data protection by design.

These ideas are mostly philosophical at the moment (and let's face it, they sound quite idealistic), but there are already AI development projects in this direction on the market, such as SingularityNET, developed to create a decentralized AI.[67]

However, as the above quote from a science fiction scenario also underlines, this technology can also be used to build institutions that are capable of fundamentally and seriously affecting human society. In the series Westworld, an AI entity with highly accurate data on the personalities and habits of all the inhabitants of Earth can foresee human fates and therefore seeks to influence lives invisibly through information society services provided to humans, effectively depriving humanity of free will. Although, according to the story, this AI runs on a centralized system, so its activity can be easily influenced or even stopped compared to a blockchain-based distributed system. A blockchain-based AI would be much more robust, yet also more transparent. Nevertheless, the impact and risks posed on those affected, i.e. humans, would be quite serious. This is why it is important to start a scientific discourse on the compliance of such systems with data protection law early on. I hope I have contributed to this dialogue through my study.

---

[65] Skalex. (2020) *AI and Blockchain: The intersection of top tech trends* [blog entry]. Available from: https://www.skalex.io/artificial-intelligence-blockchain/ [Accessed 13 February 2021].

[66] Banafa, A. (2019) *Blockchain and AI: A Perfect Match?* [blog entry]. Available from: https://www.bbvaopenmind.com/en/technology/artificial-intelligence/blockchain-and-ai-a-perfect-match/ [Accessed 13 February 2021].

[67] Member of the project team, Arif Khan, said: *"Think of blockchain as a broad horizontal layer that embraces different cultures, nations and geographical areas. Everyone can have access to this horizontal layer and interact with technology that allows people to add and work with very different sets of data. Compared to centrally managed datasets, blockchain-based databases are not controlled by any central entity."* Quotes: Wolfson, R. (2018) *Diversifying Data with Artificial Intelligence and Blockchain Technology* [press release, interview]. Available from: https://www.forbes.com/sites/rachelwolfson/2018/11/20/diversifying-data-with-artificial-intelligence-and-blockchain-technology/#407937894dad [Accessed 13 February 2021].

LIST OF REFERENCES

[1] Andrássy, G. (2008) *Philosophy and Legal Ethics.* Dialog Campus, Pécs.

[2] Article 29 Data Protection Working Party. (2017) *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679* (WP251rev.01). Available from: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 [Accessed: 8 February 2021].

[3] Attila Péterfalvi et. al. (2018) *Magyarázat a GDPR-ról (Interpretation of the GDPR*). Budapest: Wolters Kluwer.

[4] Bacon, J. et. al. (2017) *Blockchain Demystified*. Queen Mary School of Law Legal Studies Research Paper No. 268/2017.

[5] Banafa, A. (2019) *Blockchain and AI: A Perfect Match?* [blog entry]. Available from: https://www.bbvaopenmind.com/en/technology/artificial-intelligence/blockchain-and-ai-a-perfect-match/ [Accessed 13 February 2021].

[6] Buterin, V. (2013) *A Next-Generation Smart Contract and Decentralized Application Platform*. Available from: https://ethereum.org/en/whitepaper [Accessed 14 February 2021].

[7] Cauer, E. et. al. (2000) Life and Work of Wilhelm Cauer (1900 – 1945). *Proceedings of the Fourteenth International Symposium of Mathematical Theory of Networks and Systems (MTNS2000)*.

[8] Commission nationale de l'informatique et des libertés (CNIL) (2017). *How can humans keep the upper hand? The ethical matters raised by algorithms and artificial intelligence.* Available from: https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf [Accessed 23 July 2021].

[9] Datatilsynet. (2018) *Artificial intelligence and privacy.* Available from: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf [Accessed 8 February 2021].

[10] European Central Bank. (2017) *How could new technology transform financial markets?* 19th April 2017. [online]. Available from: www.ecb.europa.eu/explainers/tell-me-more/html/distributed_ledger_technology.en.html [Accessed 08 February 2021].

[11] European Commission. (2012) *Recommendation on preparations for the roll-out of smart metering systems (2012/148/EU) 9 March 2012*. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32012H0148& [Accessed: 15 December 2021].

[12] European Data Protection Board. (2020) *Guidelines on consent under Regulation (EU) 2016/679.* Available from: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf [Accessed 30 December 2020].

[13] European Union Agency for Fundamental Rights (2019) *Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights.* Available from: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf [Accessed 22 July 2021].

[14] Filatova, N. (2020) Smart contracts from the contract law perspective: outlining new regulative strategies, *International Journal of Law and Information Technology*, Volume 28, Issue 3, Autumn 2020. Available from: https://doi.org/10.1093/ijlit/eaaa015 [Accessed 14 February 2021].

[15] Finck, M. (2019) Blockchain and the General Data Protection Regulation. *European Parliamentary Research Service,* PE 634.445.

[16] Frankenfield, J. (2021) *Merkle Root (Cryptocurrency).* Available from: https://www.investopedia.com/terms/m/merkle-root-cryptocurrency.asp [Accessed 22 December 2021].

[17] Győrfi, A. et. al. (2019) *Kriptopénz ABC (Cryptocurrency ABC).* Budapest: HVG Books.

[18] Hungarian National Authority for Data Protection and Freedom of Information. (2017) *Opinion on Blockchain Technology in the Context of Data Protection (18th July 2017)* [online]. Available from: https://naih.hu/data-protection/decisions [Accessed 08 February 2021].

[19] Infostart. (2018) *Belenéztek a fekete dobozba az ELTE kutatói (Researchers of Eötvös Lóránd University looked into the black box)* [press release]. Available from: https://infostart.hu/tudomany/2018/11/16/melytanulasi-halozatot-vizsgaltak-az-elte-kutatoi [Accessed 13 February 2021].

[20] Jung, C. G. (2017) *The collected works of C.G. Jung, Part 9/I.: The archetypes and the collective unconscious.* Budapest: Scolar.

[21] Kachorowska, M. (2019) Blockchain-based land registration: Possibilities and challenges. *Masaryk University Journal of Law and Technology*, Vol. 13. No. 2. Available from: https://doi.org/10.5817/MUJLT2019-2-8 [Accessed 13 February 2021].

[22] Kakavand, H. et. al. (2017) *The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies.* Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849251 [Accessed 13 February 2021].

[23] Lopes, V. and Alexandre, L. A. (2019) An Overview of Blockchain Integration with Robotics and Artificial Intelligence. *Ledger Journal* Vol. 4, Supplement 1 (2019): Proceedings of the First Symposium on Blockchain and Robotics, MIT Media Lab, Cambridge, MA, 5 December 2018, USA. Available from: https://doi.org/10.5195/ledger.2019.171 [Accessed 23 July 2021].

[24] Mannan, R. et. al. (2019) GDPR and Blockchain: A Compliance Approach. *European Data Protection Law Review* 3/2019.

[25] McMurren, J. et. al. (2018) *Adressing Transaction Costs Through Blockchain and Identity in Swedish Land Transfers*. Available from: blockchan.ge/blockchange-land-registry.pdf [Accessed 13 February 2021].

[26] Pokol, B. (2018) *A mesterséges intelligencia társadalma (Society of Artificial Intelligence).* Budapest: Kairosz.

[27] Pokol, B. (2018) *Artificial Intelligence: The Emergence of a New Layer of Being? (AI in the Mirror of Nicolai Hartmann's Ontology).* Available from: http://dx.doi.org/10.2139/ssrn.3225111 [Accessed 13 February 2021].

[28] Sandner P. et. al. (2020) Convergence of Blockchain, IoT, and AI, Front. *Blockchain* 3:522600, Available from: https://doi.org/10.3389/fbloc.2020.522600 [Accessed 11. November 2021.].

[29] Sankaran, S. et. al. (2018) Towards Realistic Energy Profiling of Blockchains for Securing Internet of Things. *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)* Vienna.

[30] Schrepel, T. (2021) *Smart Contracts and the Digital Single Market Through the Lens of "Law + Technology" Approach*. European Commission. Available from: https://ssrn.com/abstract=3947174 [Accessed 26 December 2021].

[31] Skalex. (2020) *AI and Blockchain: The intersection of top tech trends* [blog entry]. Available from: https://www.skalex.io/artificial-intelligence-blockchain/ [Accessed 13 February 2021].

[32] Szabo, N. (1996) *Smart Contracts: Building Blocks for Digital Markets*. Available from: www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf [Accessed 8 February 2021].

[33] Szepesvári, C. (2005) Machine learning – a brief introduction. [lecture]. *MTA SZTAKI.* Available from: http://old.sztaki.hu/~szcsaba/talks/lecture1.pdf [Accessed 9 February 2021].

[34] Veale, M. and Edwards, L. (2018) Clarity, surprises and further questions in the Article 29 Working Party draft guidance on automated decision making and profiling. *Computer, Law and Security Review* 34.

[35] Verbeek A. and Lundquist M. (2021) *Artificial intelligence, blockchain and the future of Europe: How disruptive technologies create opportunities for a green and digital economy.* Available from: https://op.europa.eu/en/publication- detail/-/publication/8730fef5-315c-11ec-bd8e-01aa75ed71a1/language-en [Accessed 21 December 2021].

[36] Wolfson, R. (2018) *Diversifying Data with Artificial Intelligence and Blockchain Technology [press release, interview].* Available from: https://www.forbes.com/sites/rachelwolfson/2018/11/20/diversifying-data-with-artificial-intelligence-and-blockchain-technology/#407937894dad [Accessed 13 February 2021].

[37] Xing, B. and Marwala, T. (2018) *The Synergy of Blockchain and Artificial Intelligence.* Available from: http://dx.doi.org/10.2139/ssrn.3225357 [Accessed 13 February 2021].

DOI 10.5817/MUJL2022-1-4

EU COMMON POSITION ON INTERNATIONAL LAW AND CYBERSPACE[1]

by

ANNA-MARIA OSULA, AGNES KASPER, ALEKSI KAJANDER[*]

The discussion on international law applicable to cyber operations has shifted from asking whether international law applies to cyberspace to how it applies. Recently the European Union declared in its renewed cybersecurity strategy the ambition to develop common EU position on the application of international law in cyberspace. As part of a broader vision in striving for leadership on standards, norms and regulatory frameworks in cyberspace, the joint communication underlined the need for taking a more proactive stance in the discussions at the United Nations and other relevant international fora. However, less than half of the European Union Member States have issued a public statement on the interpretation of international law in cyberspace and hence, reaching a consensus on the interpretation of relevant concepts of international law appears a challenge. This article provides an overview of the current status of European Union Member States' public statements on international law applicable to cyber operations, identifies the domains of international law where convergence of views can be observed and highlights the areas with notable differences.

[1] Anna-Maria Osula's research for this article was supported by the Masaryk University ERDF project "Cyber Security, Cyber Crime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01 / 0.0 / 0.0 / 16_019 / 0000822). The contribution by Agnes Kasper is part of the cooperation within Jean Monnet Network "European Union and the Challenges of Modern Society" (611293-EPP-1-2019-1-CZ-EPPJMO-NETWORK). The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects only the views of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

[*] anna-maria.osula@taltech.ee; Senior researcher at Tallinn University of Technology; Research fellow at Masaryk University.

agnes.kasper@taltech.ee; Senior lecturer at Tallinn University of Technology.

aleksi.kajander@taltech.ee; Early stage researcher at Tallinn University of Technology.

KEY WORDS

European Union, International law, Cyber norms, Cyber security, United Nations, Cyberspace, Cyber law

1. INTRODUCTION

International law, norms, confidence- and capacity-building form the backbone for current discussions aiming at building and maintaining trust and security in the digital environment. International law forms the foundation for stability and predictability between states as it reflects common views of accepted state behaviour. International law also offers options for legal responses to cyber operations targeted against a state. In particular, adherence to international law plays an important role in protecting small nations who lack military power or resources.[2] Arguably, the predictability provided by international law may potentially act as deterrence against possible malicious cyber operations.

By now, the discussion on international law has shifted from asking *whether* international law applies to cyberspace to *how* it applies.[3] With some exceptions (such as the Council of Europe Budapest Convention on Cybercrime), there are no international agreements currently tailored specifically for regulating state behaviour in cyberspace. Therefore, state practice and national declarations on how states interpret international law applicable to cyber operations are valuable for increased legal certainty and transparency. However, currently only a fairly limited number of states have published comprehensive views on international law in cyberspace.[4]

With individual countries hesitating to publish national views, regional and international organisations have the potential to facilitate discussions and provide platforms for reaching a consensus. So far, few international organisations have successfully reached a consensus among their members on aspects of international law and cyberspace (such as the UN and NATO which will be discussed below). Many others have simply expressed their general support on the applicability of international law in cyberspace.[5]

However, recently the European Union (EU) declared in its renewed cybersecurity strategy the ambition to develop a common EU position

---

[2] Osula, A. (2021) *'Aligning Estonian and Japanese Efforts in Building Norms in Cyberspace', So Far, Yet So Close: Japanese and Estonian Cybersecurity Policy Perspectives and Cooperation*. Tallinn: International Centre for Defence and Security, p. 23.

on the application of international law in cyberspace. As part of a broader vision of striving for leadership on standards, norms and regulatory frameworks in cyberspace, the joint communication underlined the need for taking a more proactive stance in the discussions at the UN and other relevant international fora. Moreover, it emphasized that the EU is best placed to "*advance, coordinate and consolidate Member States' positions in international fora*".[6]

Against this backdrop the aim of the article is to give an overview of the current status of EU MSs' public statements on international law applicable to cyber operations, identify the domains of international law where convergence of views can be observed and highlight the areas with

[3] EU has an unwavering position regarding the applicability of international law in cyberspace. Equally, the applicability of human rights in cyberspace is uncontroversial among the EU MSs and there is consensus that human rights law applies online the same as it does offline. See E.g. Ministry for Foreign Affairs and International Cooperation (2021) *Italian Position Paper on 'International Law and Cyberspace'.* Rome: Ministry for Foreign Affairs and International Cooperation. Available from: https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf [Accessed 7 January 2022],p. 10. Austria (2020). *Pre-draft Report of the OEWG – ICT Comments by Austria.* Available from: https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-austria.pdf [Accessed 14 January 2022], pp. 3-4. United Nations General Assembly (2021) *Official compendium of voluntary national contributions on the subject of how international technologies by States submitted by participating government experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established pursuant to General Assembly resolution 73/266.* New York: United Nations General Assembly. Available from: https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf [Accessed 14 January 2022], p. 78. Government of the Kingdom of Netherlands (2019) *Appendix: International law in cyberspace*. Available from: https://www.government.nl/binaries/government/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf [Accessed 7 January 2022, p. 5, Slovenia (2021) *Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, Informal virtual meeting (18, 19 and 22 February 2021) Slovenia Statement*. Available from: https://front.un-arm.org/wp-content/uploads/2021/02/Slovenia-19-February-2021-FINAL.pdf [Accessed 14 January 2022], p. 2., Ministry of Foreign Affairs of Finland (2020) *International law and cyberspace Finland's national positions.* [online] Available from: https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727 [Accessed 7 January 2022], pp. 7-8, Estonia (2021) *Estonian contribution on the subject of how international law applies to the use of information and communications technologies by states, to be annexed to the report of the Group of Governmental Experts on Advancing responsible state behaviour in cyberspace (2019-21).* Available from: https://ccdcoe.org/uploads/2018/10/Estonian_contribution_on_international_law_to_the_gge_may_2021_English.pdf [Accessed 14 January 2022], p. 5. See also NATO (2020) *Allied Joint Publication-3.20 Allied Joint Doctrine for Cyberspace Operations*. Brussels: NATO Standardization Office, 19.

[4] From the EU countries, citing the most recent ones; Austria (2020) op. cit., Estonia (2021) op. cit, Government of the Kingdom of Netherlands (2019) op. cit., Czech Republic (2020) op. cit., Italy: Ministry for Foreign Affairs and International Cooperation (2021) op. cit., Romania: United Nations General Assembly (2021A) op. cit., pp. 75-79, Germany: The Federal Government (2021) op. cit., France: Ministere Des Armees (2019) op. cit., Finland: Ministry of Foreign Affairs of Finland (2020) op. cit.

notable differences. As such the article seeks to provide useful analysis for the future endeavours of the EU in fulfilling the objective set in 2020.

2. INTERNATIONAL DISCUSSIONS ON INTERNATIONAL LAW

Before analysing individual EU MS's interpretation of international law applicable to cyber operations, it is relevant to review the extent of a common position formed on other international fora, namely the UN and NATO, as this can offer a useful starting point for identifying pan-EU communalities. Such analysis also points out the areas where the interpretations of EU MSs rest upon the consensus reached on international fora, and where they have been further elaborated upon.

The UN is the most active platform for discussing norms for states in cyberspace. Since 1998, when the Russian Federation first introduced a draft resolution on information security in the First Committee of the UN General Assembly,[7] the UN Secretary-General has been issuing annual reports with the views of UN MSs to the General Assembly (GA).[8] Groups of Governmental Experts (GGEs) have been formed in 2004/5, 2009/10, 2012/13, 2014/15, 2016/17 and 2020/21 with the total of four consensus reports (in 2010, 2013, 2015, 2021) to examine the existing and potential threats from the cyberspace and possible cooperative measures to address them.[9] Notably, the 2015 UN GGE report was adopted also as the GA

[5] E.g. Organization of American States (2021) *AG/RES. 2959 (L-O/20) International Law.* Washington: Organization of American States. Available from: http://www.oas.org/en/sla/iajc/docs/AG-RES_2959_EN.pdf [Accessed 14 January 2022]; Association of Southeast Asian Nations (2018) *ASEAN Leaders' Statement on Cybersecurity Cooperation*, Singapore: Association of Southeast Asian Nations. Available from: http://setnas-asean.id/site/uploads/document/document/5b04cdc25d192-asean-leaders-statement-on-cybersecurity-cooperation.pdf [Accessed 14 January 2021] and G20 (2015) *G20 Leaders' Communiqué Antalya Summit, 15-16 November 2015*. Anatalaya:G20, Available from: https://www.gpfi.org/sites/gpfi/files/documents/G20-Antalya-Leaders-Summit-Communiqu--.pdf [Accessed 14 January 2022].

[6] European Commission (2020) *Joint Communication to the European Parliament and the Council the EU's Cybersecurity Strategy for the Digital Decade*. Brussels: European Commission. Available from: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 [Accessed 20 January 2022], p. 20.

[7] United Nations General Assembly (1999) *Resolution Adopted by the General Assembly [on the report of the First Committee (A/53/576).* New York: United Nations General Assembly. Available from: https://undocs.org/en/A/RES/53/70 [Accessed 14 January 2022].

[8] United Nations Office for Disarmament Affairs. *Developments in the field of information and telecommunications in the context of international security.* New York: United Nations Office for Disarmament Affairs. Available from: https://www.un.org/disarmament/ict-security/ [Accessed 14 January 2022].

resolution 70/237, calling all MSs to „*be guided in their use of information and communications technologies by the 2015 report of the [GGE].*"[10]

Although the 2010 UN GGE consensus report did not directly address international law, the following GGE reports have established the essential role of international law in reducing risks to international peace, security and stability. In 2013 the GGE consensus report put forward the landmark position that "*international law and in particular the [UN] Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment*" and included a set of recommendations on norms, rules and principles of responsible behaviour by states.[11] The 2015 GGE report featured a specific section on how international law applies to the use of ICTs and mentioned several international law concepts relevant to state behaviour in cyberspace.[12] The 2021 GGE report expanded the consensus even further by, *inter alia*, underlining the applicability of international humanitarian law in cyberspace and pleading countries not to conduct and support cyber operations targeting critical infrastructure, including the technical infrastructure essential for the Internet and health sector entities. Over the years, the UN GGE has invited its participating governmental experts to provide voluntary national contributions about how international law applies to the use of ICTs by states.[13]

---

[9] The UN GGE convened in 2009 and 2016 did not reached consensus report. However, reports were published in 2010 (A/65/201), 2013 (A/68/98*) and 2015 (A/70/174). United Nations Office for Disarmament Affairs (2019) *Fact Sheet Developments in the field of information and telecommunications in the context of international security*. New York: United Nations Office for Disarmament Affairs. Available from: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf [Accessed 14 January 2022].

[10] United Nations General Assembly (2015A) *Resolution adopted by the General Assembly on 23 December 2015 [on the report of the First Committee (A/70/455) 70/237*. New York: United Nations General Assembly. Available from: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/457/57/PDF/N1545757.pdf?OpenElement [Accessed 14 January 2022].

[11] United Nations General Assembly (2013) *Resolution adopted by the General Assembly on 23 December 2015 [without reference to a Main Committee (A/68/L.26 and Add. 1)] 68/98*. New York: United Nations General Assembly. Available from: https://undocs.org/A/RES/68/98 [Accessed 14 January 2022].

[12] United Nations General Assembly (2015B) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. New York: United Nations General Assembly. Available from: https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 [Accessed 14 January 2021].

[13] E.g. the 2021 report included the opinions of 15 countries in United Nations General Assembly (2021A) op. cit.

In addition to the GGE process, the UN Open-Ended Working Group (OEWG) also concluded a consensus report in 2021.[14] The report set a precedent by reflecting the discussions held among all UN MSs and *inter alia* focused on how international law applies to the use of ICTs by states. The final text offered broad support to the framework for responsible state behaviour, the general applicability of international law as well as norms developed by the previous efforts of the UN GGE, notably the GGE 2015 report.

As an important development, the North Atlantic Treaty Organisation NATO has published in 2020 an *Allied Joint Doctrine for Cyberspace Operations* (hereafter AJP-3.20) which reflects the (almost) consensus of 30 NATO members. The document is intended primarily as guidance for NATO commanders, staffs and forces while also providing guidance for NATO Members, partners, non-NATO nations and other organisations. The document clearly states that the adopted framework sets out the parameters within which its military forces can operate and that international law provides prescriptions and limitations for both forces and individuals.[15]

While it is important to note that the reports adopted by the UN GGE and OEWG are not law-making processes *per se*, they still have a significant role to play in pinpointing legal concepts supported and valued internationally, and thereby shaping and establishing international agreement on accepted state behaviour in cyberspace. Equally, the AJP-3.20 does not only reflect an agreement among a military organisation, but also indicates a common view of 21 EU MSs which is an indication of larger convergence of views among EU MSs than what can be deduced from analysing individual domestic positions.

---

[14] United Nations General Assembly (2021B) *Open-ended working group on developments in the field of information and telecommunications in the context of international security*. New York: United Nations General Assembly. Available from: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf [Accessed 14 January 2022].

[15] NATO (2020) op. cit., pp. xiii, 20, 22. See also Schmitt, M. (2020) *Noteworthy Releases of International Cyber Law Positions – Part I: NATO*, New York: Lieber Institute West Point. Available from: https://lieber.westpoint.edu/nato-release-international-cyber-law-positions-part-i/ [Accessed 14 January 2022].

3. COMMON THEMES IN THE EU MEMBER STATES' OFFICIAL VIEWS

Our research has identified public statements pertaining to the interpretation of international law and cyber operations, or mentioning related concepts, from the majority of EU MSs. However, in most of these cases, the identified documents were broadly worded and did not go into detail with legal discussions. Nevertheless, we determined nine EU MSs' declarations, all referenced to in this article, to be more extensive and thereby useful in shedding light to the scope of the EU MSs' common and diverging views. It must be underlined that the national positions we have analysed are in many aspects much more nuanced then referenced below, while at the same time it has been challenging to assess the meaning of some aspects which have (deliberately or not) not been mentioned in the positions.

In addition to national positions, we have also considered the UN GGE and OEWG reports, related EU documents and the AJP-3.20 publication. Given that the UN GGE 2015 report has been endorsed by the UN GA, we view this document as reflecting the broad consensus of UN MSs. The OEWG report and AJP-3.20 reflect respectively the consensus of the UN and NATO members.

3.1 SOVEREIGNTY

Sovereignty is no doubt one of the most politically loaded terms in the discussions revolving around state behaviour in cyberspace. The relevance of the concept of sovereignty in cyberspace has been endorsed in the UN GGE and OEWG reports and mentioned by all nine EU MSs who have published their more detailed legal views.

In the debate on whether sovereignty should be considered as principle[16] of international law or a principle *and a* standalone rule, the breach of which would entail an internationally wrongful act, the EU MSs' approach appears rather unified. AJP-3.20 includes a reference to sovereignty as a rule,[17] thereby reflecting the common position of twenty one EU MSs

[16] For the UK position see: Wright, J. (2018) *Cyber and International Law in the 21st Century*. London: Chatham House. Available from: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century [Accessed 14 January 2022]

[17] NATO (2020) op. cit., p. 20, footnote 26.

who also belong to NATO, making the total number of EU MSs having expressed support for sovereignty as a rule twenty three.

For example, and in the aftermath of the foiled cyberattack targeting the OPCW, the Netherlands was one of the firsts in September 2019 to state publicly that "*respect for the sovereignty of other countries is an obligation in its own right, the violation of which may in turn constitute an internationally wrongful act*".[18] About the same time, France also issued an elaborate document detailing its interpretations of the international law applicable to cyber operations and made clear that it may consider certain cyberattacks against French digital systems or any effects produced on French territory by digital means a breach of sovereignty as long as state attribution can be established – hence violation of sovereignty as a rule is conceivable.[19] Estonia[20], Austria[21], Finland[22], Czech Republic[23], Germany[24], Romania[25] and Italy[26] followed in suit, all agreeing that sovereignty entails both rights and obligations, and essentially, that violation of sovereignty by a cyber operation is capable of being an internationally wrongful act. These positions are summarised below in Chart 1.

---

[18] Government of the Kingdom of Netherlands (2019) op. cit., p. 2.

[19] Ministere Des Armees (2019) *International Law Applied To Operations in Cyberspace*. Paris: Delegation a l'information et a la communication de la defense. Available from: https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf [Accessed 7 January 2022].

[20] ERR News (2019) *President Kaljulaid at CyCon 2019: Cyber attacks should not be easy* weapon. Tallinn: ERR News. Available from: https://news.err.ee/946827/president-kaljulaid-at-cycon-2019-cyber-attacks-should-not-be-easy-weapon [Accessed 14 January 2022]. Also in United Nations General Assembly (2021) op. cit., p. 26.

[21] Austria.(2020) op. cit., p. 3.

[22] Ministry of Foreign Affairs of Finland (2020) op. cit., p. 7.

[23] Czech Republic (2020) *Czech Republic Statement by Mr. Richard Kadlcak Special Envoy for Cyberspace Director Cyberseuciryt Department at the 2nd substantive session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security of the First Committee of the General Assembly of the United Nations*. New York: United Nations General Assembly. Available from: https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf [Accessed 14 January 2022], p. 3.

[24] The Federal Government (2021) *On the Application of International Law in Cyberspace*. Berlin: German Federal Foreign Office. Available from: https://ccdcoe.org/uploads/2018/10/Germany_on-the-application-of-international-law-in-cyberspace-data_English.pdf [Accessed 7 January 2022], p. 3.

[25] United Nations General Assembly (2021A) op.cit., p. 76.

[26] Ministry for Foreign Affairs and International Cooperation (2021) op.cit., p. 4.

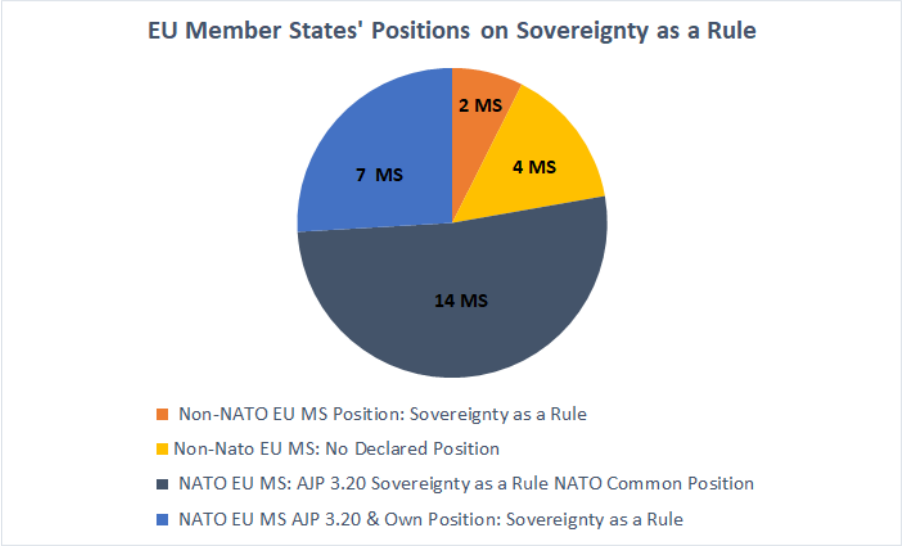

Chart 1.

Based on the EU MSs' positions, the most supported approach is that sovereignty is a principle and rule, entailing both rights and obligations. Its components are internal and external sovereignty, and they also apply in cyberspace. The authority of the state to exercise sovereignty is not unlimited. Cyber operation attributable to a state that causes non-negligible harmful tangible impact on the territory of the target state will likely violate territorial sovereignty.

All EU MSs' positions distinguish between internal and external aspects of sovereignty, but some chose to emphasize or simply limit its position to a specific aspect in their general discussion of sovereignty. The German and Czech positions remain closely linked to territory and effects caused therein, and the Netherlands elaborates in detail on internal sovereignty. Taking a somewhat different route, Romania focuses on immaterial dimensions, Finland brings specific examples illustrating that a "*state possesses a legal interest in the protection of its territory from any form of external harmful action*".[27] France[28], Finland[29] and Estonia[30] use wordings that leave the door open to consider cyber operations where the targeted infrastructure is located outside their territory (e.g. in case of use of cloud

[27] Ministry of Foreign Affairs of Finland (2020) op. cit., p. 2 referring to Nuclear Tests (Australia v. France), Judgment, I.C.J. Reports 1974, p. 253, para. 456.

[28] Ministere Des Armees (2019) op. cit., p. 7.

[29] Ministry of Foreign Affairs of Finland (2020) op. cit., p. 2.

[30] United Nations General Assembly (2021A) op. cit., p. 24.

services). A particularly clear position is formulated by France, whereas France "*exercises jurisdiction over information systems located in its territory*" and adds in a footnote that also over "*connected objects /.../ and content operated or processed via electronic communication networks which cover the national territory or from an IP address attributed to France*"[31].

What constitutes a violation depends on the characteristics of the operation in question, and case-by-case assessment is needed. Estonia briefly notes that "*[v]iews on what constitutes a breach of sovereignty in cyberspace differ. Malicious cyber operations can be complex, cross several jurisdictions and may not always produce physical effects on targeted infrastructure*"[32], leaving the discussion of the threshold for a later opportunity. Romanian and Italian positions are also non-specific, the former reaffirming that interference with or preventing the state from exercising its sovereign prerogatives can be considered breach of sovereignty[33], the latter "*considers that the principle in question prohibits a [s]tate from conducting cyber operations, which produce harmful effects on the territory of another [s]tate, irrespective of the physical location of the perpetrator*"[34].

Some states go further. For the Netherlands, the nature and consequences entail "*1) infringement upon the target [s]tate's territorial integrity; and 2) there has been an interference with or usurpation of inherently governmental functions of another [s]tate*", concurring with the Tallinn Manual in this respect.[35] Germany hints that interference with the political independence of a state, absent coercion, may in certain circumstances also constitute a breach of sovereignty, but it sets a de minimis limit to necessary *physical effects and functional impairments* that can be deemed to constitute violation of *territorial* sovereignty[36]. Czech Republic[37] and Finland too make it clear that in addition to material harm as a qualifier for breach of territorial sovereignty, loss of functionality can also be a base for claiming violation of sovereignty. In addition, Finland holds that relevant considerations include operations with the effect below the threshold of loss

[31] Ministere Des Armees (2019) op. cit., p. 6.
[32] United Nations General Assembly (2021A) op. cit., p. 25.
[33] United Nations General Assembly (2021A) op. cit., p. 76.
[34] Ministry for Foreign Affairs and International Cooperation (2021) op. cit., p. 4.
[35] Government of the Kingdom of Netherlands (2019) op. cit., p. 3.
[36] The Federal Government (2021) op. cit., p. 4.
[37] Czech Republic (2020) op. cit., p. 3.

of functionality, i.e. modification or deletion of information belonging to the target state, or to private actors in its territory.[38]

Finally, France first defines the term cyberattack[39], then it considers that any such cyberattack attributable to a state, against French digital systems or effects produced on French territory by digital means constitutes at least breach of sovereignty[40]. It appears that for France, even a failed cyberattack that does not cause any actual harm or effect, could still constitute breach of sovereignty, since the criteria set has two main elements: the operation 1) qualifies as a cyberattack under the definition; and 2) is attributable to a state. One should note here that cyber operations *intended to* cause damage or which *may* cause harm[41] also fall under the definition. The French position seems to set the lowest threshold, from the ones under scrutiny here, and the nature of the operation is the major determinant for considering what constitutes violation of sovereignty.

3.2 DUE DILIGENCE

Due diligence has been touched upon in the GGE 2015 consensus report in two occasions. Firstly, as a principle according to para. 13 (c) states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs. Secondly, but in a much narrower formulation, the principle is also recognizable in the section addressing international law, in para. 28 (e) under which states must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-state actors to commit such acts.[42]

Nine EU MSs' positions considered due diligence, hence it is a key issue, closely linked to the principle of sovereignty and state responsibility, however the modalities of application in cyberspace are less than straightforward.

Netherlands, Germany, Italy, Romania and Finland refer to the ICJ's Corfu Channel judgment, confirming the binding nature of the due diligence rule. However, France and Estonia point to the 2015 GGE report

[38] Ministry of Foreign Affairs of Finland (2020) op. cit., p. 2.

[39] Ministere Des Armees (2019) op. cit., p. 6. footnote 7. Cyberattack is "deliberate, offensive and malicious action taken via cyberspace that is intended to cause damage (in terms of availability, integrity or confidentiality) to information or the systems that process it and that may harm the activities of which it or they are the medium".

[40] Ministere Des Armees (2019) op. cit., p. 7.

[41] Ministere Des Armees (2019) op. cit., p. 6, footnote 7.

[42] United Nations General Assembly (2021A) op. cit.

para. 13 (c), where due diligence *principle* in a non-binding format is set out, which countries *should* follow; nevertheless, these states also use a language that indicates the binding nature of the due diligence. France posits that it is a customary obligation[43], while Estonia uses the wording that "*states have to make reasonable efforts to ensure that their territory is not used to adversely affect the rights of other states*". [44] Austria literally underlines that "*[s]tates must seek to ensure that their territory is not misused for the commission of internationally wrongful acts using ICTs*".[45]

Majority of positions[46] point out or imply by their language that it is an obligation of conduct, not result, and that "*knowledge*"[47] is a constitutive element of the obligation to arise. However, a few remain silent on both matters, therefore conclusions can be drawn only with these limitations. Compliance with this obligation is by taking feasible or reasonable measures when another state suffers consequences of certain gravity. While numerous states hint that feasibility, or what can be considered reasonable, is a variable standard[48], contextual[49] and can depend on the various capabilities of the state in question[50], no common position can currently be deducted from those. The precise cyber threshold for triggering the due diligence obligation also remains unclear, but there seems to be a tendency to argue that the consequences need to be sufficiently adverse, but not necessarily in the form of physical damage.[51] Yet only few refer to a positive obligation to protect human rights explicitly as a trigger for due diligence obligation.[52]

Generally, the aim of such due diligence measures is to prevent or halt harmful activities, their consequences on the target state or activities which

---

43 Ministere Des Armees (2019) op. cit., p. 6.

44 United Nations General Assembly (2021A) op. cit., p. 26. Emphasis added.

45 Austria (2021) *Comments by Austria on the Zero-Draft for the OWEG's Final Report*. Available from: https://front.un-arm.org/wp-content/uploads/2021/02/Austria-Comments-Zero-Draft-OEWG-19.02.2021.pdf [Accessed 14 January 2022].

46 Estonia (2021) op. cit., Government of the Kingdom of Netherlands (2019) op. cit., Ministry for Foreign Affairs and International Cooperation (2021) op. cit., United Nations General Assembly (2021) op. cit.

47 Ibid.

48 Ministry of Foreign Affairs of Finland (2020) op. cit., p. 4.

49 Government of the Kingdom of Netherlands (2019) op. cit., p. 5.

50 Estonia (2021) op. cit., p. 26, Government of the Kingdom of Netherlands (2019) op. cit.

51 Government of the Kingdom of Netherlands (2019) op. cit., p. 5.

52 Ministry of Foreign Affairs of Finland (2020) op. cit., p. 5; Ministry for Foreign Affairs and International Cooperation (2021) op. cit., p. 6.

carry the risk of causing significant transboundary harm.[53] However, the term "*prevention*" in this context usually refers to an obligation relating to ongoing or imminent operations, and essentially means to stop them or their consequences.[54] Estonia offered a more progressive view on this point, linking the due diligence principle with capacity building, and proposing that "*[s]tates should strive to develop means to offer support, when requested by the injured state, to identify or attribute malicious cyber operations*"[55].

Finally, while other states also mention potential violations of due diligence obligation, France pays more attention to this question, expressing that a "*state's failure to comply with this obligation is not a ground for an exception to the prohibition of the use of force*".[56]

3.3 INTERVENTION

Whereas the UN GGE 2021[57] and 2015[58] reports mention the principle of non-intervention, it is not included in the OEWG report nor in AJP-3.20. Based on our research seven EU MSs have publicly shared their views on prohibited intervention.

It is generally agreed that the obligation of non-intervention prohibits states from intervening coercively in the internal or external affairs of other states. Even though the obligation of non-intervention is not explicitly mentioned in the UN Charter, it can be derived as a corollary of the sovereignty principle, Article 2(1) of the UN Charter and is grounded in customary international law. Germany is of the opinion that cyber measures may constitute a prohibited intervention under international law if they are comparable in scale and effect to coercion in non-cyber contexts.[59]

In broad terms, all the seven countries agreed that for an act to qualify as a prohibited intervention, it must fulfil two main conditions. Firstly, the act must bear on those matters in which states may decide freely, or in other words, interfere with the *domaine réservé of* another state. Secondly, the act must be coercive in nature.

---

53 Ministry of Foreign Affairs of Finland (2020) op. cit, p. 4.

54 Coco, A. Dias, T. (2021) *'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law*. European Journal of International Law, Vol 32(3), p. 787.

55 United Nations General Assembly (2015B) op. cit., p. 26.

56 Ministere Des Armees (2019) op. cit., p. 10.

57 United Nations General Assembly (2021A) op. cit., pp. 70, 71(c).

58 United Nations General Assembly (2015B) op. cit., pp. 26, 28(b).

59 The Federal Government (2021) op. cit., p. 5.

However, the definition of „*coercion*" remains unsettled among EU MSs. Some of the countries underline that an act involves coercion if its internal processes regarding aspects pertaining to its *domaine réservé* are significantly influenced and the act is specifically designed to compel the victim state to change its behaviour with respect to a matter within its *domaine réservé*.[60] Germany brings an example of a state spreading disinformation via the internet, and thereby deliberately inciting violent political upheaval, riots and/or civil strife in a foreign country, and thus significantly impeding the orderly conduct of an election and the casting of ballots.[61] Tampering with elections is also mentioned by other states.[62]

Others remain more cautious and state that for an act to include coercion, it should effectively deprive the target state of its ability to control or govern matters within its *domaine réservé.*[63] Here France brings an example: "*Interference by digital means in the internal or external affairs of France, i.e. interference which causes or may cause harm to France's political, economic, social and cultural system, may constitute a violation of the principle of non-intervention.*"[64]

However, it is generally accepted that merely influencing the other state by persuasion or propaganda, providing harsh criticism or causing nuisance with the aim of attempting to achieve a certain behaviour from the other state does not qualify as coercion.[65] Moreover, the acting state must intend to intervene in the internal affairs of the target state.[66] Finally, there has to be a causal nexus between the coercive act and the effect on the internal or external affairs of the target state.[67]

---

[60] Ibid. United Nations General Assembly (2021A) op. cit., pp. 25, 57. Ministry for Foreign Affairs and International Cooperation (2021) op. cit., pp. 4-5. Tallinn Manual 2.0, commentary to rule 66, para 19. Finland's approach to this issues is "*…done with the purpose of compelling or coercing that State in relation to affairs regarding which it has free choice (so-called domaine réservé)*„ Ministry of Foreign Affairs of Finland (2020) op. cit., p. 3.

[61] The Federal Government (2021) op. cit., p. 5.

[62] United Nations General Assembly (2021A) op. cit., pp. 25, 57, 77. Ministry of Foreign Affairs of Finland (2020) op. cit., p. 3. Ministry for Foreign Affairs and International Cooperation (2021) op. cit., p. 5.

[63] Schmitt, M. (2017) op. cit., p. 318.

[64] Ministere Des Armees (2019) op. cit., p. 7.

[65] The Federal Government (2021) op. cit., p. 5. Ministry of Foreign Affairs of Finland (2020) op. cit., p. 3.

[66] The Federal Government (2021) op. cit., p. 5.

[67] United Nations General Assembly (2021A) op. cit., p. 77. Schmitt, M. (2017) op. cit., p. 320, para 24 (the exact nature of the causal nexus was not agreed on).

3.4 COUNTERMEASURES

The baseline view which can be deduced to be the opinion of minimum 21 EU MSs derives from AJP-3.20, which acknowledges countermeasures as legal remedies.[68] Apart from AJP-3.20, seven EU MSs have publicly expressed their views on the topic. Countermeasures are not mentioned in the UN GGE and OEWG reports.

All seven EU MSs echo the understanding expressed in AJP-3.20: that injured states have the right to take proportionate[69] countermeasures under international law in response to an internationally wrongful act. Such measures would otherwise be unlawful under international law. Several additional elements related to the interpretation of the legal regime on countermeasures are mentioned below.

Germany, Italy and France point out that the response to a wrongful cyber operation may involve digital means or not.[70] Netherland brings an example of a countermeasure: "*a cyber operation could be launched to shut down networks or systems that another state is using for a cyberattack*".[71] France states that in the event of a cyberattack against its information systems, state agencies may conduct cyberoperations, and "*on a case-by-case basis, and on a decision by the national cyber defence chain, such operations may be carried out in the framework of counter-measures*".[72]

All countries refer to limitations related to countermeasures. Italy, France and Estonia point out that countermeasures can be employed in response to internationally wrongful acts below the armed attack threshold. Netherlands posits that countermeasures are subject to strict conditions.[73] Italy, Estonia, Germany, Finland and France add that countermeasures are limited to the purpose of ensuring compliance with breached obligations.[74] Equally, Italy, Finland, Netherlands and France confirm that countermeasures must not amount to a threat, or use, of force

---

[68] NATO (2020) op. cit., footnote 36.

[69] E.g. in the wording of France: „*commensurate with the injury suffered, taking into account the gravity of the initial violation and the rights in question*". Ministere Des Armees (2019) op. cit., p. 8.

[70] Ministere Des Armees (2019) op. cit., p. 8. The Federal Government (2021) op. cit., p. 13.

[71] United Nations General Assembly (2021A) op. cit., p. 62.

[72] Ministere Des Armees (2019) op. cit., p. 8.

[73] Government of the Kingdom of Netherlands (2019) op. cit., p. 63.

[74] Ministry of Foreign Affairs of Finland (2020) op. cit., p. 5. Ministry for Foreign Affairs and International Cooperation (2021) op. cit., p. 7. Ministere Des Armees (2019) op. cit., p. 7. United Nations General Assembly (2021A) op. cit., p. 29. The Federal Government. (2021). op. cit., p. 13.

and must be consistent with other peremptory norms, as well as with human rights and humanitarian law.[75]

Countries also bring out issues which can be seen as challenging. Italy and France point out that "*the victim-[s]tate is generally required to call upon the [s]tate of origin to discontinue the wrongful act and to notify it of its intention to take countermeasures in response to wrongful cyber operations*", however, such requirement may not apply if immediate action is needed to enforce the rights of the injured state and to prevent further damage.[76] Netherland agrees that "*if immediate action is required in order to enforce the rights of the injured state and prevent further damage, such notification may be dispensed with*".[77] Italy also states that countermeasures may be problematic due to, for example, difficulties of "*traceability, assessment of breach in relation with the threshold of the diligence due, significance of the harm suffered.*"[78] Germany explains that "*[d]ue to the multifold and close interlinkage of cyber infrastructures not only across different [s]tates but also across different institutions and segments of society within [s]tates, cyber countermeasures are specifically prone to generating unwanted or even unlawful side effects. Against this background, [s]tates must be particularly thorough and prudent in examining whether or not the applicable limitation criteria to cyber countermeasures are met.*"[79]

Netherlands, Germany and Estonia underline the requirement that the injured state invoke the other state's responsibility, i.e. that the internationally wrongful act be attributed to a state.[80] Finland agreed with the importance of having adequate proof (which generally does not have to be disclosed) on the source of the offensive operation and state responsibility before resorting to countermeasures, while admitting that in certain circumstances it may be possible to attribute the hostile operation only afterwards.[81] The latter may be seen in contradiction with

[75] Ministry of Foreign Affairs of Finland (2020) op. cit., p. 5. Government of the Kingdom of Netherlands (2019) op. cit., p. 63. Ministere Des Armees (2019) op. cit., p. 8.

[76] Ministere Des Armees (2019) op. cit., p. 8.

[77] Government of the Kingdom of Netherlands (2019) op. cit., p. 63.

[78] Ministry for Foreign Affairs and International Cooperation (2021) op. cit., p. 7.

[79] The Federal Government (2021) op. cit., p. 3, 64.

[80] United Nations General Assembly (2021A) op. cit., pp. 29-30, 63. The Federal Government (2021) op. cit., p. 13.

[81] Ministry of Foreign Affairs of Finland (2020) op. cit., p. 6.

the understanding that countermeasures should normally be taken while the wrongful act is ongoing.[82]

Estonia has expressed the view that among other collective responses, states which are not directly injured may apply collective countermeasures to support the state directly affected by the malicious cyber operation, while underlining that countermeasures applied should follow the principle of proportionality and other principles established within the international customary law.[83] France disagrees and states that "*collective counter--measures are not authorised*".[84] AJP-3.20 reflects the difference of opinions and posits that "*it is an unsettled area of the law whether international organisations or other states may conduct countermeasures on behalf of an injured state for unlawful acts that occur below the threshold of an armed attack.*"[85]

3.5 STATE RESPONSIBILITY AND ATTRIBUTION

State responsibility and attribution are complex issues which are sparking different opinions on the international arena. The 2015 and 2021 UN GGE reports affirmed that states must meet their international obligations regarding internationally wrongful acts attributable to them under international law.[86] This reflects a general understanding that when a state's cyber operation violates its obligations under international law, it constitutes an internationally wrongful act under the law of state responsibility. Internationally wrongful acts require two elements: 1) attributability to the state under international law, and 2) breach of an international obligation of the state.[87]

The 2015 and 2021 UN GGE reports also affirmed that states must not use proxies to commit internationally wrongful acts using ICTs and that the indication that an ICT activity was launched or otherwise originates

---

[82] Ibid.

[83] ERR News (2019) op. cit.

[84] Ministere Des Armees (2019) op. cit., p. 7.

[85] NATO (2020) op. cit.

[86] United Nations General Assembly (2015B) op. cit., 28 (f); United Nations General Assembly (2021C) *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. New York: United Nations General Assembly. Available from: https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf [Accessed 14 January 2022] 71 (g).

[87] International Law Commission (2001) *Report of the International law Commission on the work of its fifty-third session, 23 April-1 June and 2 July – 10 August 2001, Official Records of the General Assembly, Fifty-sixth session, Supplement No.10.* Geneva: International Law Commission. Available from: https://legal.un.org/ilc/documentation/english/reports/a_56_10.pdf [Accessed 20 January 2022], Article 2.

from the territory or the ICT infrastructure of a state may be insufficient in itself to attribute the activity to that state.[88] This is expanded by several EU MSs who add that state responsibility can be established if the cyber operation was carried out by a state organ, a person or entity exercising elements of governmental authority, or non-state actor while being under instruction, direction or control by a state.[89]

Regarding attribution, the baseline EU approach is settled in the EU Cyberdiplomacy toolbox which outlines the core principles such as 1) not all measures require attribution; 2) attribution is a sovereign political decision by a state; 3) EU MSs can coordinate attribution at EU level. According to the EU, attribution could be established, based on an analysis of technical data and all-source intelligence, including on the possible interests of the aggressor. It must be noted that there is no international legal obligation to reveal evidence on which attribution is based prior to taking an appropriate response. MSs may employ different methods and procedures to attribute malicious cyber activities and different definitions and criteria to establish a degree of certainty on attributing a malicious cyber activity.[90]

Importantly, the application of the regime of targeted restrictive measures by the EU does not amount to attribution, which is a sovereign political decision taken on a case-by-case basis.[91] The UN GGE 2021 report adds that invocation of the responsibility of a state for an internationally wrongful act involves complex technical, legal and political considerations.[92]

Several EU MSs emphasize that there is no requirement for the state to make a public attribution.[93] France underlines that "*a decision not to publicly attribute a cyberattack is not a final barrier to the application*

[88] United Nations General Assembly (2015B) op. cit., 28 (e)(f); United Nations General Assembly (2021C) op. cit., 71 (g).

[89] United Nations General Assembly (2021A) op. cit., pp. 28, 61-62, 78-79. Ministere Des Armees (2019) op. cit., p. 10. The Federal Government (2021) op. cit., p. 11. underlining „effective control"; Finland mentions .. /.../ if acting on behalf of the State" Ministry of Foreign Affairs of Finland (2020) op. cit., p. 5.

[90] Council of the European Union. (2017) *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activity*. Brussels: Council of the European Union. Available from: https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf [Accessed 14 January 2022].

[91] Council of the European Union (2019) *Council Decision* concerning restrictive measures against cyber-attacks threatening the Union or its Member States. Brussels: Council of the European Union. Available from: https://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf [Accessed 14 January 2022]

[92] United Nations General Assembly (2021C) op. cit., 71 (g).

of international law, and in particular to assertion of the right of response available to [s]tates".[94]

3.6 INTERNATIONAL HUMANITARIAN LAW

There is consensus among EU MSs that International Humanitarian Law (IHL) applies to cyber operations during armed conflicts, which is the same position as put forth in the UN GGE 2021[95] as well as in AJP-3.20.[96] However, there are differing views primarily on neutrality, distinction between military and civilian objects and when a cyber operation constitutes an attack under IHL. Nevertheless, for the most part the EU MSs view the applicability of IHL in cyberspace during a conflict in a similar manner, which is perhaps not surprising as all EU MSs are parties to the four Geneva Conventions and at least Additional Protocols I and II.

Eleven EU MSs[97] have stated their views on the applicability of IHL to cyber operations during armed conflicts, out of which, three (Finland, Austria, and Ireland) are not NATO members. Out of these three, only Finland has published a detailed document on their national position[98], and while Ireland has stated its intention to release a similar document, currently their more detailed views on the subject are not known beyond that IHL applies in cyberspace.[99] Therefore, while silent NATO and EU MSs may be assumed agree with the AJP-3.20, the same cannot be said for the non-NATO members. Consequently, the "*silent*" non-NATO EU MSs

---

93 Ministere Des Armees (2019) op. cit., p. 10. Ministry of Foreign Affairs of Finland (2020) op. cit., p. 6. Ministry for Foreign Affairs and International Cooperation (2021) op. cit., p. 5. United Nations General Assembly (2021A) op. cit., pp. 28, 61. The Federal Government (2021) op. cit., p. 12.

94 Ministere Des Armees (2019) op. cit., p. 11.

95 United Nations General Assembly (2021C) op. cit., p. 18.

96 NATO (2020) op. cit., p. 19.

97 Note that Ireland and Slovenia have expressed their view on this particular matter but have otherwise not published a detailed interpretation of international law applicable to cyber operations. Austria (2020) op. cit., pp. 2-3. Czech Republic (2020) op. cit., p. 4. Estonia (2021) op. cit., p. 1. Ministere Des Armees (2019) op. cit., p. 4, Ministry of Foreign Affairs of Finland (2020) op. cit., p. 7, The Federal Government (2021) op. cit., p. 1, Department of Foreign Affairs (2021) *Statement by Minister Coveney at the UNSC Open Debate on Cyber Security*. [online]. Available from: https://www.dfa.ie/pmun/newyork/news-and-speeches/securitycouncilstatements/statementsarchive/statement-by-minister-coveney-at-the-unsc-open-debate-on-cyber-security.html [Accessed 7 January 2022], Ministry for Foreign Affairs and International Cooperation (2021) op. cit., p. 9. Slovenia (2021) op. cit., p. 2, United Nations General Assembly (2021A) op. cit., pp. 77-78, Government of the Kingdom of Netherlands (2019) op. cit., p. 5.

98 Ministry of Foreign Affairs of Finland (2020) op. cit.

99 Department of Foreign Affairs (2021) op. cit.

that have not explicitly stated their interpretations remain an unknown variable.

Another point of divergence is perceptible on dual-use objects, where France has a slightly different interpretation to AJP-3.20, the Tallinn Manual 2.0 (TM) and other EU MSs. Under the AJP-3.20, if an entity has both military and civilian uses ("*dual use*"), a "*careful analysis must be carried out to determine if they constitute a lawful military objective*" through losing their classification as a civilian object "*or otherwise offer a definite military advantage*".[100] This interpretation mirrors TM Rule 102 whereby if there is doubt regarding cyber infrastructure that is "*normally dedicated to civilian purposes*" being used to make an "*effective contribution to military action*" a determination of military use "*may only be made following a careful assessment*".[101] The disagreement flows from the ambiguity of whether Article 52 (3) of AP I, which contains a presumption of civilian usage, reflects customary law, with TM concluding that such a presumption only applies to individuals as noted in Rule 95 of the TM based upon Article 50 (1) of AP I.[102]

Considering that not all NATO MSs are party to Additional Protocol I, such as the United States[103], it unsurprising that AJP-3.20 mirrors the compromise wording of the TM. France in its national position upholds the presumption of Article 52 (3) of AP I, whereby in case of doubt, objects (just as individuals under 50 (1)) are presumed not to be used to "*make an effective contribution to military action*".[104] France emphasises its disagreement with the TM interpretation[105], and hence by extension, with the AJP-3.20. However, considering that the AJP-3.20 was published after the French national position, it remains to be seen if France continues to maintain its position. By contrast, Germany explicitly confirms that they agree with the TM Rule 102 regarding the careful assessment.[106]

---

[100] Op. cit., p. 21.

[101] Schmitt, M. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, p. 448.

[102] Ibid, p. 424.

[103] International Committee of the Red Cross. *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.* [online]. Available from: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/States.xspxp_viewStates=XPages_NORMStatesParties&xp_treatySelected=470 [Accessed 7 January 2022).

[104] Ministere Des Armees (2019) op. cit., p. 14.

[105] Ibid.

[106] The Federal Government (2021) op. cit., p. 8.

Similarly, the qualification of data has been subject to discussion. France, Finland[107], Romania[108] and Germany[109] provided converging opinions whereby data, although intangible, may become a protected object or military objective, through the principle of distinction. France, for example, considers that „*the special protection afforded to certain objects extends to systems and the data that enable them to operate*"[110] and carved out some examples. Accordingly, „*given the current state of digital dependence, content data (such as civilian, bank or medical data, etc.) are protected under the principle of distinction*".[111] There was no opposing view in the positions reviewed, however states approach this issue cautiously.

Furthermore, France disagrees with the TM on the definition of a cyberattack, as under the French interpretation, a cyber operation may be classified as an attack under Article 49 of AP I even if there is no injury or loss of life or physical damage.[112] Instead, it is enough if the object is no longer able to provide the service it was intended for.[113] The German position mirrors the sentiment, albeit less overtly, as they do not explicitly state that they reject the TM's interpretation.[114] The German definition refers to "*harmful effects on communication, information or other electronic systems*" as well as "*or on physical objects or persons*", and thus mirroring the French interpretation whereby the physical damage, to either objects or persons, is not required.[115]

The Finnish position does not explicitly define a "*cyberattack*", but rather states that a cyberattack may amount to use of force under Article 2 (4) of the UN Charter or "*armed attack*" under Article 51 based on its consequences.[116] The Finnish position does not therefore explicitly either affirm or contradict the TM's Rule 92.[117] AJP-3.20 does not provide an exact definition of a cyberattack, as the discussion is focused mainly on when a "*cyber operation*" (which includes cyberattacks) would amount

[107] Ministry of Foreign Affairs of Finland (2020) op. cit., p. 7.
[108] United Nations General Assembly (2015B) op. cit.
[109] The Federal Government (2021) op. cit., p. 8.
[110] Ministere Des Armees (2019) op. cit., p. 15.
[111] Ibid, p. 14.
[112] Ibid, p. 13.
[113] Ibid.
[114] The Federal Government (2021) op. cit., p. 8.
[115] Ibid.
[116] Ministry of Foreign Affairs of Finland (2020) op. cit., p. 6.
[117] Ibid.

to an "*armed attack*" or "*use of force*". Therefore, there is not a definite consensus on the definition of a "*cyberattack*", and whether physical damage is required for a cyber action to be considered a cyberattack among the EU MS.

The final major point of divergence is the application of the law of neutrality. AJP-3.20 leaves it for the individual state to interpret and apply the law of neutrality.[118] There appears to be consensus, among the available positions of France, Italy, the Netherlands and Romania that the law of neutrality applies in cyberspace,[119] however, there is disagreement of what it entails. While it is agreed that neutral territory must be respected, by refraining from harming any infrastructure located on such territory, or using it to launch attacks, there is disagreement whether the neutral state must deny *any* access to its ICT infrastructure.

France considers that while a state may allow the belligerents to use its ICT network for communication, it must otherwise prevent "any use" of its ICT infrastructure.[120] By contrast, Italy emphasizes neutrality in treatment, whereby "*any action*" by a neutral state must be "*equally applied to all belligerents*", with an example that a state may not provide or deny access to its ICT infrastructure to one party only.[121] The Dutch position makes a similar statement,[122] whereby it can be concluded that there are two distinct positions on the topic, one for treating all belligerents equally and the French position of only allowing communication to pass through its ICT infrastructure and otherwise preventing any use of its ICT infrastructure by the belligerents. Considering there are relatively few positions available on the topic, as only four EU MSs have expressed their views, this specific issue lacks agreement.

3.7 USE OF FORCE

Among the EU MSs examined, there is a similar interpretation of the applicability of the prohibition on the use of force enclosed in Article 2(4) of the UN Charter. The examined EU MSs generally agree that cyber

[118] NATO (2020) op. cit., p. 22.

[119] Ministere Des Armees (2019) op. cit., p. 16, United Nations General Assemblv (2021A) op. cit., p. 78. Ministry for Foreign Affairs and International Cooperation (2021) op. cit., p. 10, Government of the Kingdom of Netherlands (2019) op. cit., p. 5.

[120] Ministere Des Armees (2019) op. cit., p. 16.

[121] Ministry for Foreign Affairs and International Cooperation (2021) op. cit., p. 10.

[122] Government of the Kingdom of Netherlands (2019) op. cit., p. 5.

operations may amount to "*use a force*" based on the consequences ("*scale and effect*") of the cyber operation, with the means being unimportant. There is also broad support to the interpretation that a cyber operation with sufficiently severe consequences may amount to not only a "*use of force*" but also an "*armed attack*", the latter being the gravest form of "*use of force*", thereby upholding an appreciable distinction.

AJP-3.20 interpretation is effectively the same, whereby cyber operations may amount to a use of force, or an "*armed attack*" if grave enough based on their scale and effect.[123] However, there is disagreement over whether a cyber operation that lacks material damage can amount to a "*use of force*", which is reflected in the careful wording of AJP-3.20. AJP-3.20 agrees that cyber operations "*generally would not*" amount to a "*use of force*" if they only create "*temporary disruptions or denials of service*".[124] Moreover, AJP-3.20 mentions that if part of a wider concurrent conventional attack, cyber operations that in isolation would not amount to a "*use of force*" such as a "*temporary denial of service*", could be classified as an "*armed attack*".[125] Thus, there is room for interpretation, albeit the doctrine appears to cautiously agree that a mere temporary loss of functionality on its own would not be sufficient, thereby mirroring the TM approach.[126]

France continues to uphold the view that material damages are not required, and that loss of functionality could be sufficient for a cyber operation to be deemed a "*use of force*".[127] France's position contains an interesting contradiction to both the TM and the *Nicaragua* case upon which the former's view was based on. The TM considers that "*merely funding*" a hacktivist group "*would not be a use of force*"[128], which mirrors the case's determination whereby a "*mere supply of funds /.../ does not in itself amount to a use of force*".[129] However, the *Nicaragua* judgement considers "*training and arming*" to "*certainly /.../ involve the threat or use of force*". Contrastingly, France posits that the "*financing or even training individuals to carry out cyberattacks against France*" may be seen as an example of a "*use*

[123] NATO (2020) op. cit., p. 20.
[124] Ibid.
[125] Ibid.
[126] Schmitt, M. (2017) op. cit., p. 337.
[127] Ministere Des Armees (2019) op. cit., p. 7.
[128] Schmitt, M. (2017) op. cit., p. 331.
[129] Judgement of 27 June 1986, *Nicaragua v. United States of America*. International Court of Justice, paragraph 228.

of force".[130] Therefore, France's national position subtly appears to communicate its disagreement with the Court's view in the *Nicaragua* case, by suggesting that training, arming and funding are all equivalent levels of action in terms of the "*use of force*" classification.

In Italy's view, which was published after AJP-3.20, the matter remains unresolved as it is stated that the notion that cyber operations which "*merely cause loss of functionality*" is "*a controversial one*".[131] Nevertheless, Italy does consider that due to the "*reliance of modern societies on computers*", the "*interruption of essential services*" which would not necessarily require physical damage, could justifiably be considered a "*use of force*".[132] Consequently, it is reasonable to conclude that while there is no definitive consensus on whether "*a mere*" loss of functionality may amount to a "*use of force*", such an interpretation *could* be justifiable in the opinion of at least some EU MSs.

3.8 SELF-DEFENCE

Majority of the EU MSs agree that the right to self-defence under Article 51 of the UN Charter applies in cyberspace and that cyber operations may amount to an armed attack that enables a state to exercise the said right.[133] Similarly, there is no apparent controversy over collective self-defence or responding to a cyber operation amounting to an armed attack via conventional kinetic means, provided they are necessary and proportionate.[134] However, controversies exist regarding exercising self-defence against non-state actors whose actions are not on behalf of any state and whether very severe non-material consequences of a cyber operation may amount to an armed attack.

The extension of the right to self-defence to non-state actors whose actions are not on behalf of any state, is arguably the most divisive of the controversial topics on self-defence. France outright rejects such an extension to non-state actors acting on their own accord, despite

[130] Ministere Des Armees (2019) op. cit., p. 7.

[131] Ministry for Foreign Affairs and International Cooperation (2021) op. cit., p. 8.

[132] Ibid.

[133] Government of the Kingdom of Netherlands (2019) op. cit., pp. 8-9, The Federal Government (2021) op. cit., pp. 15-16, Ministrv of Foreign Affairs of Finland (2020) op. cit., pp. 6-7., Ministere Des Armees (2019) op. cit., pp. 6, 8. Estonia (2021) op. cit., pp. 7, 8-9, Ministry for Foreign Affairs and International Cooperation (2021) op. cit., p. 9, NATO. (2020) op. cit., p. 20.

[134] Ibid.

in "*exceptional cases*" taking self-defence measures against "*quasi-[s]tate*" non-state actors such as ISIS.[135] However, it must be noted that France included the caveat of "*general practice*" which is shifting the interpretation of the law of self-defence, whereby self-defence against such non-state actors may become authorised.[136]

By contrast, Germany considers that non-state actors can commit "*armed attacks*", with reference to its views on the acts of Al-Qaeda and ISIS[137], in which it considered that states taking actions against such non-state actors are acting in self-defence.[138] Therefore, Germany appears to support the extension of self-defence to non-state actors acting on their own accord. The topic, however, appears to be a difficult one, for Finland avoids taking a definitive position. Despite stating that the right to self-defence arises from an armed attack attributed to a particular state, the attached footnote clarifies that non-state actors may possibly be capable of armed attacks, but the "*related questions of self-defence*" against such actors are "*too complicated to be discussed here*".[139]

Another issue of controversy lies with the thresholds for an armed attack. The German position lists as relevant factors only items that relate to material damages or injuries, including indirect deaths, as well as serious territorial incursions.[140] However, the French position also points out that a cyber operation may be categorised as an armed attack if it also causes "*substantial*" economic damage.[141] The Dutch position remains uncommitted as they refer to a lack of international consensus in the case of a lack of "*fatalities, physical damage or destruction*" but with "*very serious non-material consequences*" which seemingly could include economy damage.[142] The Italian position refers to cyberattacks comparable to conventional attacks that cause "*disruption in the functioning of critical infrastructure*"[143], and thereby not explicitly mentioning the economic consequences. Finland raises the question on how should the indirect and long-term impacts

[135] Ministere Des Armees (2019) op. cit.
[136] Ibid.
[137] The Federal Government (2021) op. cit., p. 16.
[138] Letter dated 10 December 2015 from the Chargé d'affaires a.i. of the Permanent Mission of Germany to the United Nations addressed to the President of the Security Council.
[139] Ministry of Foreign Affairs of Finland (2020) op. cit., p. 7.
[140] The Federal Government (2021) op. cit., p. 15.
[141] Ministere Des Armees (2019) op. cit., p. 8.
[142] Government of the Kingdom of Netherlands (2019) op. cit., p. 9.
[143] Italy: Ministry for Foreign Affairs and International Cooperation (2021) op. cit., p. 9.

of the cyber operation be considered in the case of potential classification as an armed attack.[144]

Therefore, the issue of economic damage amounting to an armed attack remains controversial. Moreover, further discussions about the extent to which long-term and indirect impacts of cyber operations when they are being classified as a potential armed attack appear to be warranted, as currently there is considerable uncertainty.

4. CONCLUSION

The goal of this article has been to give an overview of the current status of EU MSs' public statements on international law applicable to cyber operations, identify the domains of international law where convergence of views can be observed and, in some instances, also highlight some areas with notable differences.

The analysis of EU MSs' legal positions and relevant international documents (especially taking into account the AJP-3.20) revealed that while only nine out of twenty-seven EU MSs have published their detailed official views on the interpretation of international law applicable to cyber operations, there appears to be more consensus between the countries than evident at first sight. The EU MSs are heading towards a common position in many areas, and that beyond what has been agreed in the UN already. In addition to the already long-established strong standpoints on the general applicability of international law to state behaviour in cyberspace and the foundational role of human rights, the following baselines can be identified:

A) The relevance of the concept of sovereignty in cyberspace has been endorsed in the UN GGE and OEWG reports and mentioned by all nine EU MSs who have published their more detailed legal views. Considering the consensus reflected in AJP-3.20, there seems to be a broad agreement among 23 EU MSs regarding the interpretation of sovereignty as a standalone rule, entailing both rights and obligations.
B) Nine EU MSs' positions considered due diligence as a key issue, closely linked to the principle of sovereignty and state

[144] Ministry of Foreign Affairs of Finland (2020) op. cit, p. 6.

responsibility; however, the modalities of the application of the concept in cyberspace remain less than straightforward. The broad idea that countries should not knowingly support cyber operations has been expressed also in the UN GGE and OEWG reports, despite not employing the term "*due diligence*".

C) Seven EU MSs have publicly shared their views on prohibited intervention. It is generally agreed that the obligation prohibits states from intervening coercively in the internal or external affairs of other states. In broad terms, all the seven EU MSs agreed that for an act to qualify as a prohibited intervention, it must fulfil two main conditions. Firstly, the act must bear on those matters in which states may decide freely, or in other words, interfere with the *domaine réservé of* another state. Secondly, the act must be coercive in nature. The UNGGE 2021 and 2015 reports also mention the principle of non-intervention but do not go into greater detail.

D) The baseline view which can be deduced to be the opinion of 22 EU MSs is that countermeasures are acknowledged as legal remedies. Al seven EU MSs who have separately expressed their views echo the AJP-3.20 general position in outlining that injured states have the right to take proportionate countermeasures under international law in response to an internationally wrongful act. Such measures would otherwise be unlawful under international law. AJP-3.20 posits that collective countermeasures remain an unsettled area of the law.

E) State responsibility and attribution are complex issues which are sparking different opinions on the international arena. The 2015 and 2021 UN GGE reports affirmed that states must meet their international obligations regarding internationally wrongful acts attributable to them under international law, thereby also reflecting the de minimis agreement among the EU. The EU's baseline approach to attribution is outlined by the Cyberdiplomacy Toolbox.

F) Majority of the EU MSs agree that the right to self-defence under Article 51 of the UN Charter applies in cyberspace and that cyber operations may amount to an armed attack that enables a state to exercise the said right. Similarly, there is no apparent controversy over collective self-defence or responding to a cyberoperation

amounting to an armed attack via conventional kinetic means, provided they are necessary and proportionate.

G) The general consensus that IHL applies to cyber operations during armed conflicts, as confirmed by the UN GGE 2021 report, is supplemented by separate mentions in the domestic positions of several EU MSs. IHL-related questions are also addressed in the AJP-3.20, but many open issues remain.

However, drawing more concrete conclusions on the EU MSs' interpretation of international law applicable to cyber operations is limited due to the majority of EU MSs not having published their positions. It should be also underlined that national positions vary one the level of detail and include several blanks where the country's positions are not clearly expressed or in some instances, certain topics not mentioned at all. Therefore differences in national positions or states' silence on certain topics do not necessarily or not always signify oppositions. At the same time, lack of detail in discussing certain concepts may refer to strategic omissions which reflect domestic objectives and principles.

To move forward with the goal of a unified EU position, we suggest a three-step approach: a) clarifying domestic views, b) determining the common denominator, and c) engaging EU MSs in wider political discussions aimed at reaching decisions on a common EU position. However, drawing up a national position on the application of international law to cyber operations is not a trivial exercise. Although the overwhelming majority of EU MSs now show interest and engage in the UN discussions on international peace and security in the context of the use of ICT, it is likely that a more proactive stance could be advanced by targeted capacity building in this specific area. The European External Action Service (EEAS) already has some tools for this, and the European Security and Defence College offers several cyber-related courses to its network, but it still lacks a comprehensive and regular training on international law and cyber operations. Furthermore, besides the cyber-policy entrepreneur MSs, the EEAS could also intensively use all its relevant mandates to promote discussion and coordinate efforts in developing a common EU position.

And finally, there are topics where we can observe clear-cut oppositions where a common EU approach is unlikely in the near future. Examples include collective countermeasures, details related to IHL such as law of neutrality and the classification of "*use of force*" and "*armed attack*".

While reaching a substantial global agreement on different issues related to international law in cyberspace may not be viable in the near future, groups of like-minded countries such as the EU should continue working on their respective approaches. This may be seen as leading to certain fragmentation, but it also serves as an opportunity for building partnerships and synergies which will eventually drive further the discussions on international venues and serve as a role model for other regions.

LIST OF REFERENCES

[1] Association of Southeast Asian Nations (2018) *ASEAN Leaders' Statement on Cybersecurity Cooperation*, Singapore: Association of Southeast Asian Nations. Available from: http://setnas-asean.id/site/uploads/document/document/5b04cdc25d192-asean-leaders-statement-on-cybersecurity-cooperation.pdf [Accessed 14 January 2022].

[2] Austria (2021) *Comments by Austria on the Zero-Draft for the OWEG's Final Report*. Available from: https://front.un-arm.org/wp-content/uploads/2021/02/Austria-Comments-Zero-Draft-OEWG-19.02.2021.pdf [Accessed 14 January 2022].

[3] Coco, A. Dias, T. (2021) *'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law*. European Journal of International Law, Vol 32(3).

[4] Council of the European Union (2017) *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activity*. Brussels: Council of the European Union. Available from: https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf [Accessed 14 January 2022].

[5] Council of the European Union (2019) *Council Decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States. Brussels: Council of the European Union.* Available from: https://data.consilium.europa.eu/doc/document/ST- 7299-2019-INIT/en/pdf [Accessed 14 January 2022].

[6] Czech Republic (2020) *Czech Republic Statement by Mr. Richard Kadlcak Special Envoy for Cyberspace Director Cyberseuciryt Department at the 2nd substantive session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security of the First Committee of the General Assembly of the United Nations*. New York: United Nations General Assembly. Available from: https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf [Accessed 14 January 2022].

[7] Department of Foreign Affairs (2021) *Statement by Minister Coveney at the UNSC Open Debate on Cyber Security*. [online]. Available from: https://www.dfa.ie/pmun/newyork/news-and-speeches/securitycouncilstatements/statementsarchive/statement-by-minister-coveney-at-the-unsc-open-debate-on-cyber-security.html [Accessed 7 January 2022].

[8] ERR News (2019) *President Kaljulaid at CyCon 2019: Cyber attacks should not be easy* weapon. Tallinn: ERR News. Available from: https://news.err.ee/946827/president-kaljulaid-at-cycon-2019-cyber-attacks-should-not-be-easy-weapon [Accessed 14 January 2022].

[9] Estonia (2021) *Estonian contribution on the subject of how international law applies to the use of information and communications technologies by states, to be annexed to the report of the Group of Governmental Experts on Advancing responsible state behaviour in cyberspace (2019-21).* Available from: https://ccdcoe.org/uploads/2018/10/Estonian_contribution _on_international_law_to_the_gge_may_2021_English.pdf [Accessed 14 January 2022].

[10] European Commission (2020) *Joint Communication to the European Parliament and the Council the EU's Cybersecurity Strategy for the Digital Decade*. Brussels: European Commission. Available from: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 [Accessed 20 January 2022].

[11] G20 (2015) *G20 Leaders' Communiqué Antalya Summit, 15-16 November 2015*. Anatalaya:G20, Available from: https://www.gpfi.org/sites/gpfi/files/documents/G20-Antalya-Leaders-Summit-Communiqu--.pdf [Accessed 14 January 2022].

[12] Government of the Kingdom of Netherlands (2019) *Appendix: International law in cyberspace*. Available from: https://www.government.nl/binaries/government/ documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf [Accessed 7 January 2022].

[13] International Committee of the Red Cross *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.* [online]. Available from: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/States.xsp?xp_viewStates=XPages_NORMStatesParties&xp_treatySelected=470 [Accessed 7 January 2022].

[14] International Law Commission (2001) *Report of the International law Commission on the work of its fifty-third session, 23 April-1 June and 2 July – 10 August 2001, Official Records of*

the General Assembly, Fifty-sixth session, Supplement No.10. Geneva: International Law Commission. Available from: https://legal.un.org/ilc/documentation/english/reports/a_56_10.pdf [Accessed 20 January 2022].

[15] Judgement of 27 June 1986, *Nicaragua v. United States of America*. International Court of Justice, paragraph 228.

[16] Letter dated 10 December 2015 from the Chargé d'affaires a.i. of the Permanent Mission of Germany to the United Nations addressed to the President of the Security Council.

[17] Ministere Des Armees (2019) *International Law Applied To Operations in Cyberspace*. Paris: Delegation a l'information et a la communication de la defense. Available from: https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf [Accessed 7 January 2022].

[18] Ministry for Foreign Affairs and International Cooperation (2021) *Italian Position Paper on 'International Law and Cyberspace'.* Rome: Ministry for Foreign Affairs and International Cooperation. Available from: https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf [Accessed 7 January 2022].

[19] Ministry of Foreign Affairs of Finland (2020) *International law and cyberspace Finland's national positions.* [online]. Available from: https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727 [Accessed 7 January 2022].

[20] NATO (2020) *Allied Joint Publication-3.20 Allied Joint Doctrine for Cyberspace* Operations. Brussels: NATO Standardization Office.

[21] Nuclear Tests (Australia v. France), Judgment, I.C.J. Reports 1974.

[22] Organization of American States (2021) *AG/RES. 2959 (L-O/20) International Law.* Washington: Organization of American States. Available from: http://www.oas.org/en/sla/iajc/docs/AG-RES_2959_EN.pdf [Accessed 14 January 2022].

[23] Osula, A. (2021) *'Aligning Estonian and Japanese Efforts in Building Norms in Cyberspace', So Far, Yet So Close: Japanese and Estonian Cybersecurity Policy Perspectives and Cooperation*. Tallinn: International Centre for Defence and Security.

[24] *Pre-draft Report of the OEWG – ICT Comments by Austria.* Available from: https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-austria.pdf [Accessed 14 January 2022].

[25] Schmitt, M. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.

[26] Schmitt, M. (2020) *Noteworthy Releases of International Cyber Law Positions – Part I: NATO*, New York: Lieber Institute West Point. Available from: https://lieber.westpoint.edu/nato-release-international-cyber-law-positions-part-i/ [Accessed 14 January 2022].

[27] Slovenia (2021) *Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, Informal virtual meeting (18, 19 and 22 February 2021) Slovenia Statement*. Available from: https://front.un-arm.org/wp-content/uploads/2021/02/Slovenia-19-February-2021-FINAL.pdf [Accessed 14 January 2022].

[28] The Federal Government (2021) *On the Application of International Law in Cyberspace*. Berlin: German Federal Foreign Office. Available from: https://ccdcoe.org/uploads/2018/10/Germany_on-the-application-of-international-law-in-cyberspace-data_English.pdf [Accessed 7 January 2022], p.3.

[29] United Nations General Assembly (1999) *Resolution Adopted by the General Assembly [on the report of the First Committee (A/53/576).* New York: United Nations General Assembly. Available from: https://undocs.org/en/A/RES/53/70 [Accessed 14 January 2022].

[30] United Nations General Assembly (2013) *Resolution adopted by the General Assembly on 23 December 2015 [without reference to a Main Committee (A/68/L.26 and Add. 1)] 68/98.* New York: United Nations General Assembly. Available from: https://undocs.org/A/RES/68/98 [Accessed 14 January 2022].

[31] United Nations General Assembly (2015A) *Resolution adopted by the General Assembly on 23 December 2015 [on the report of the First Committee (A/70/455) 70/237.* New York: United Nations General Assembly. Available from: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/457/57/PDF/N1545757.pdf?OpenElement [Accessed 14 January 2022].

[32] United Nations General Assembly (2015B) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. New York: United Nations General Assembly. Available from: https://undocs.org/en/A/70/174 [Accessed 14 January 2022].

[33] United Nations General Assembly (2021A) *Official compendium of voluntary national contributions on the subject of how international technologies by States submitted by participating government experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established*

pursuant to General Assembly resolution 73/266. New York: United Nations General Assembly. Available from: https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf [Accessed 14 January 2022].

[34] United Nations General Assembly (2021B) *Open-ended working group on developments in the field of information and telecommunications in the context of international security*. New York: United Nations General Assembly. Available from: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf [Accessed 14 January 2022].

[35] United Nations General Assembly (2021C) *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. New York: United Nations General Assembly. Available from: https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf [Accessed 14 January 2022] 71 (g).

[36] United Nations Office for Disarmament Affairs (2019) *Fact Sheet Developments in the field of information and telecommunications in the context of international security.* New York: United Nations Office for Disarmament Affairs. Available from: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf [Accessed 14 January 2022].

[37] United Nations Office for Disarmament Affairs. *Developments in the field of information and telecommunications in the context of international security.* New York: United Nations Office for Disarmament Affairs. Available from: https://www.un.org/disarmament/ict-security/ [Accessed 14 January 2022].

[38] Wright, J. (2018) *Cyber and International Law in the 21st Century*. London: Chatham House. Available from: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century [Accessed 14 January 2022].

MUJLT Official Partner (Czech Republic)

ROWAN LEGAL, advokátní kancelář s.r.o.
www.rowanlegal.com/cz/

Cyberspace 2021 Partners

Vodafone Czech Republic
www.vodafone.cz

Wolters Kluwer
www.aspi.cz

Zákony pro lidi - AION CS
www.zakonyprolidi.cz

CODEXIS - ATLAS consulting
www.codexis.cz

Notes for Contributors

Focus and Scope

Masaryk University Journal of Law and Technology (ISSN on-line 1802-5951, ISSN printed 1802-5943) is a peer-reviewed academic journal which publishes original articles in the field of information and communication technology law. All submissions should deal with phenomena related to law in modern technologies (e.g. privacy and data protection, intellectual property, biotechnologies, cyber security and cyber warfare, energy law). We prefer submissions dealing with contemporary issues.

Structure of research articles

Each research article should contain a title, a name of the author, an e-mail, keywords, an abstract (max. 1 500 characters including spaces), a text (max. 45 000 characters including spaces and footnotes) and list of references.

Structure of comments

All comments should contain a title, a name of the author, an e-mail, keywords, a text (max. 18 000 characters) and a list of references.

Structure of book reviews

Each book review should contain a title of the book, a name of the author, an e-mail, a full citation, a text (max. 18 000 characters) and a list of references.

Structure of citations

Citations in accordance with AGPS Style Guide 5th ed. (Harvard standard), examples:

Book, one author: Dahl, R. (2004) *Charlie and the Chocolate Factory*. 6th ed. New York: Knopf.
Book, multiple authors: Daniels, K., Patterson, G. and Dunston, Y. (2014) *The Ultimate Student Teaching Guide.* 2nd ed. Los Angeles: SAGE Publications, pp.145-151.
Article: Battilana, J. and Casciaro, T. (2013) The Network Secrets of Great Change Agents. *Harvard Business Review*, 91(7) pp. 62-68.
Case: *Evans v. Governor of H. M. Prison Brockhill* (1985) [unreported] Court of Appeal (Civil Division), 19 June.
Citation Guide is available from: https://journals.muni.cz/public/journals/36/download/Citationguide.pdf

Formatting recommendations

Use of automatic styles, automatic text and bold characters should be omitted.
Use of any special forms of formatting, pictures, graphs, etc. should be consulted.
Only automatic footnotes should be used for notes, citations, etc.
Blank lines should be used only to divide chapters (not paragraphs).
First words of paragraphs should not be indented.
Chapters should be numbered in ordinary way – example: "5.2 Partial Conclusions".

Submissions

Further information available at https://journals.muni.cz/mujlt/about

LIST OF ARTICLES