

The Law in the Internet of Things Era between Created Opportunities and Vulnerabilities

Assistant professor **Tiberiu T. BAN**¹

Abstract

In the context of computerization and automation of most economic sectors and private life, the increase in the number of attacks on computer systems that expose personal data to unauthorized persons is alarming. It started from a hypothesis already validated in the specialized literature that properly designed security policies and procedures can prevent attacks exploiting known vulnerabilities to a satisfactory extent. However, their simple existence is not enough, these security policies and procedures must be adapted to the specifics of each computer system, with the appropriate legal support. We followed a transdisciplinary analysis that combines elements of informatics and legal regulations regarding the opportunities and vulnerabilities of smart devices, face to face with the criminal phenomenon of cyber crime aimed at the security and confidentiality of personal data. The main objective of the present study is to identify and extract 'lessons learned' regarding vulnerabilities of the Internet of Things type information systems. These 'good practices' allow the development of procedures and security policies useful in preventing computer attacks criminalized as the crime of unauthorized access to a computer system.

Keywords: information security, information privacy, security policies, processing procedures, preventing cyber-attacks.

JEL Classification: K24

DOI: <https://doi.org/10.62768/ADJURIS/2024/1/02>

Please cite this article as:

Ban, Tiberiu T., „The Law in the Internet of Things Era between Created Opportunities and Vulnerabilities”, in Pajuste, Tiina, Heliona Bellani (Miço) & Sejla Maslo Cerkic (eds.), *Legal Perspectives in the Modern Era of Technological Transformations*, ADJURIS – International Academic Publisher, Bucharest, Paris, Calgary, 2024, p. 24-38.

1. Introductory considerations

In everyday life, a user has come to rely on the computer systems that serve them. All the online activities of an ordinary user generate personal data that any marketing agency and any 'cybercriminal' can consider a valuable target, which also explains the fact that recent years have brought increasingly larger

¹ Tiberiu T. Ban - Faculty of Law, 'Bogdan Voda' University of Cluj Napoca, tiberiu.ban@gmail.com.

waves of cyber-attacks targeting personal data.

It is already universally accepted that standards regarding the protection of personal data are becoming increasingly high and impose stricter rules. The purpose of this endeavor is to provide an acceptable and reasonable degree of security, regardless of the state in which data processing takes place.

This aspect obliges companies² to carry out increasingly complex evaluation studies in order to provide guarantees that the data processing carried out complies with current standards in an international context.

The main difficulty relates to the fact that data processing is present in all areas and sectors of the economy and the daily activities of individual users, and the possibility of using new technologies should make all such processing easier, faster and more transparent, but it is often these that in reality introduce an additional series of problems relating to information security and the security of information systems, the solution of which is sometimes left to the individual user in the absence of specific uniform regulations.

The European Union has intervened over time with regulations offered to Member States to provide a common basis for the protection and security of personal data such as Directive 95/46/EC³ or for the protection of information systems such as the NIS Directive⁴ and recently the NIS Directive⁵.

In just the past few years, considering all these considerations, the European Union has adopted the General Data Protection Regulation⁶ due to the express desire to harmonize the rules imposed and respected by the member states regarding data processing. At the same time, the adoption of the GDPR had the effect of strengthening the level of confidentiality provided to the data subjects of these personal data processing activities.

In practice, over the past twenty years, the European Union has analysed the need for the alignment of the standards used by the member states when it comes to processing personal data, especially in the context where these processing activities are often online and tend to have a cross-border nature. The previously existing regulations allowed states to establish with a high degree of autonomy the level of data protection they consider appropriate and necessary to

² See P. Voigt, A. Bussche, *The EU General Data Protection Regulation (GDPR). A practical guide*, Springer International Publishing, 2017, pp. 2–7.

³ See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, repealed on 24 May 2018, available at <http://data.europa.eu/eli/dir/1995/46/oj>.

⁴ See Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of network and information security across the Union, available at <http://data.europa.eu/eli/dir/2016/1148/oj>.

⁵ See Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 NIS2 available at <https://eur-lex.europa.eu/eli/dir/2022/2555>.

⁶ See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) available at <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016R0679&from=EL>

impose on operators who carry out data processing, often in an automated manner through increasingly sophisticated computer systems.

Furthermore, the previous regulations did not provide any legal certainty in terms of the legislative framework, neither for operators nor for their representatives. For example, through Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, it was intended to implement a guarantee for the protection of the fundamental rights of individuals in the context of interstate processing of personal data between the member states of the Union. These efforts had limited effects because, having the status of a Directive, it was necessary for each of the member states to introduce these provisions into national legislation through separate legislation, such as Law 677/2001 in the case of Romania.

In practice, it was considered⁷ that Directive 95/46/EC failed to achieve its intended objectives because there was no alignment of standards among the member states regarding the protection of personal data in the European Union. Furthermore, in recent years, even the ‘EU – US Privacy Shield’ has been considered outdated and no longer provides sufficient guarantees⁸ on data transfers between the Union and the United States of America and has been formally invalidated⁹ finally by the decision of the Court (Grand Chamber) in Maximillian Schrems v Facebook Ireland Limited. This ‘Shield’ refers to the legal framework adopted by the European Commission¹⁰, which allowed entities and data controllers in the United States to obtain certification – sometimes self-offered – of compliance with a certain level of protection for personal data.

This shortcoming has been overcome by the joint efforts of the European Union and the United States. On 10.07.2023 the European Commission announced¹¹ the adoption of the ‘EU – US Data Privacy Framework’, considering that the United States of America has now succeeded in providing a level of pro-

⁷ See P. Voigt, A. Bussche, *op. cit.*, p. 2.

⁸ See Joint Press Statement by European Commissioner for Justice Didier Reynders and US Secretary of Commerce Wilbur Ross, 10.08.2020 on the assessment of a possible enhanced Privacy Shield to meet the requirements of the 16 July 2020 Judgment – Facebook v. Schrems, available at https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en accessed 15.08.2022.

⁹ See Judgment of the Court (Grand Chamber) of 16 July 2020 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. Case C-311/18. Available at <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:62018CJ0311>.

¹⁰ See Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of the EU-US Privacy Shield (notified under document number C (2016)4176, available at http://data.europa.eu/eli/dec_impl/2016/1250/oj).

¹¹ See press release ‘Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows’, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_23_3721.

tection for the processing of personal data similar to that implemented in the European Union.

2. The reality and opportunities of new technologies

The changes¹² that technology and the widespread use of information systems in all aspects of everyday life¹³ undoubtedly open up opportunities and new ways in which data can be processed. Computer systems are becoming increasingly powerful, with impressive computing power and virtually infinite data storage capacity, which is becoming increasingly economically accessible.

The last decade has been marked by a spectacular leap forward in the evolution of information and communication technology. Internet connectivity for computers has become increasingly cost-effective and faster. This has led to a transition in terms of websites and online content availability. As a first step, the transition from static web 1.0 sites to dynamic sites, user-generated content, social media platforms, and a general trend towards encouraging users to share more information, life moments, memories, and even potentially sensitive data online can be observed. Consequently, there is an essential need to pay particular attention to ensuring an adequate level of security for computer networks and component systems, considering that a vast proportion of critical systems rely on computer systems, and an attack targeting them can have devastating effects¹⁴ at the level of an entire country.

User interaction with online devices has moved beyond the computer screen to the area of mobile devices, gadgets ‘always connected’ to computer system networks or the Internet. Data storage has become much more accessible through the technological advance that cloud-based technologies have demonstrated.

As the user becomes more and more dependent on internet-connected devices, they become part of the Internet of Things ecosystem, an ecosystem of ‘smart’ devices that collect data from the user, some of which is personal data, biometric data, and other devices are given a maximum ‘trusted’ role in the private network topology, being allowed to control other devices.

Internet-connected systems offer a standard of living that we are now unwilling to give up, there is unrestricted access to information, entertainment, socialising. However, each such technological revolution brings both a number of economic and social benefits, but also allows the exploitation of new paradigms

¹² See T. Ban, *The digital future of law between the opportunities of the cyber era and the acute need for security*, in *Curierul Judiciar*, no. 6, 2020, pp. 339–345.

¹³ See A. Ciurea, *The Digital Age and Justice (I). Objectives, algorithm design methods and consequences of their use in justice*, in *Revista Universul Juridic*, No. 1 January 2022, pp. 56–70, available at http://revista.universuljuridic.ro/wp-content/uploads/2022/03/06_Revista_Universul_Juridic_nr_1-2022_PAGINAT_BT_A_Ciurea.pdf.

¹⁴ See I. VasIU, *Criminalitatea informatică*, Ed. Nemira, Bucharest, 1998, p. 139.

previously unexplored or insufficiently protected by national legislation.

As we have previously argued¹⁵, the shift to the paradigm of an almost fully digitised society comes not only with advantages but also with a new set of vulnerabilities that allow malicious individuals to exploit totally innovative ways to coordinate attacks on information systems targeting data availability, integrity or confidentiality as well. This prospect raises a number of new challenges¹⁶ for the legislator regardless of the country, as the phenomenon has a cross-border dimension due to the elements of foreignness that arise very easily in a cyber, virtual environment, where often the concrete, the geographical location of the computer systems targeted by cyber attacks is not even known.

However, although the aim is to prevent criminal phenomena directed against a computer system or using a computer system, all measures taken by the legislator must be based on respect for the principle of proportionality between interference in individual rights and freedoms – in particular the right to privacy¹⁷ to the confidentiality of communications and the seriousness of these crimes, for the good of society as a whole.

In terms of the consequences of these offences, they can range from some directed against a specific person such as accessing a social networking account to read private conversations without the right to some directed against state institutions among those involved in the effective work of combating crime in the cyber environment, such as the Romanian Police and IGPR.

It is questioned whether there are distinctions between cybercrime in terms of the status of the active subject and the possible criminal participation in terms of the possibility of finding the criminal guilt of the legal person. The legal issue of criminal liability of the legal person with its legal characteristics is a fairly recent institution introduced in Romanian legislation, which has been previously analysed under the comparative aspect of the arguments for and against the appropriateness of its introduction in the legislative framework. The Internet certainly allows the advantage of possible anonymity from the illusion of security offered by the personal computer monitor, which explains why the online area has become an early target for a new type of attackers, those specialising in attacks on information systems, with cases of famous convictions¹⁸ in American jurisprudence since the 1990s, causing colossal damage.

As a new area of crime, the need to understand this totally new criminal

¹⁵ See T. Ban, *Fraud committed through information systems and electronic means of payment – Legislative challenges of the digital age*, in Preventing and Combatting Cybercrime. The International Conference, Accent Publishing House, Cluj Napoca, 2016, pp. 264–274.

¹⁶ See Law No. 302/2004 on international judicial cooperation in criminal matters, republished in the Official Gazette Part I, No. 411 of 27 May 2019.

¹⁷ See M. C. Dănişor, *The Rule of Law – Guaranteeing Privacy in the Cyber Era*, in the Rule of Law in the Digital Era. The International Conference, Accent Publishing House, Cluj Napoca, 2016, pp. 118–136.

¹⁸ See I. Vasîu, *Hackers. Cybercriminals or rebels with a cause? (All about hackers)*, Nemira Publishing House, Bucharest, 2001, pp. 114–133.

phenomenon has arisen in order to formulate a plan to prevent such attacks. A number of theories have been formulated¹⁹ in the field of criminology related to cybercrime, in a multidisciplinary approach that allows the formulation of prevention models.

In this new domain, it is easy to understand that classical investigation models specific to the criminal prosecution phase, evidence gathering to determine judicial truth, and ultimately determining the perpetrator's identity cannot be applied. There is a fundamental need for adaptation of these investigation techniques to remote modes of operation, sometimes disguised by a series of interposed computer systems in the chain of connections from the attacker to the target computer system. Not only the sphere of criminal law needed an update and openness to new models to cope with the increasing wave of crimes committed through or against computer systems. Procedural criminal law also needed a paradigm shift regarding methods of criminal investigation²⁰ used to achieve the purpose provided for in art. 285 of the Criminal Procedure Code, namely the collection of necessary evidence, while respecting the principle of legality. This often involves the preparation of a well-elaborated and adapted investigation plan based on the actual reality of the offence that is the subject of criminal action.

Because in many situations, the evidence needed by law enforcement agencies is recorded through computer systems – sometimes even involuntarily, for example, continuous geolocation via GPS systems or network cells from mobile network operators – determining the commission of offenses under criminal law and, by extension, preventing their future commission can be achieved through specialized new methods such as those expressly provided by the legislator aimed at obtaining specific data related to internet traffic or location by collaborating with telecommunications service providers or by conducting digital searches on these systems.

Although in Romanian jurisprudence, there have been criminal cases related to the commission of illicit acts involving computer systems, they have often been initially classified as common crimes such as theft, fraud, without noting a criminal trend that would prompt the legislator to begin judicial practice establishing these acts as offenses previously incriminated before the year 2014 in special laws that transpose into Romanian legislation exactly the offenses that Romania has undertaken to incriminate through the Convention²¹ since 2001.

However, there are famous cases²² of such cases in British as well as American case law, even from the 1980s, and these can rightly be considered as

¹⁹ See A. C. Moise, *The criminological dimension of crime in cyberspace*, 2nd edition, C. H. Beck, Bucharest, 2020, pp. 67–85.

²⁰ See G. I. Ionita, *Cybercrime offences. Incriminating, investigating, preventing and combating*, 3rd edition, Universul Juridic Publishing House, Bucharest, 2018, pp. 216–222.

²¹ See European Convention on Cybercrime, Budapest, 2011.

²² See I. Vasiu, *op. cit.*, 1998, pp. 106–120.

pioneering cases for the formulation of modern criminal rules in the field of computer crime.

This makes it easier and easier for any operator to process extremely large amounts of data in an increasingly easy, fast and cost-effective way, without investing in economic know-how. All these are business opportunities, but at the same time they may also present concerns about how a satisfactory level of privacy could be ensured for personal data and thus, in the perspective of the GDPR Regulation (EU) 2016/679, all the rights of the data subjects of such processing could be respected.

Online activities are becoming the de facto standard of service for users, offering solutions that rely on revolutionary technologies such as cloud computing, social media, advertising and targeted promotion based on customer behaviour.

It is also necessary that in situations where controllers carry out special activities involving the processing of very large amounts of data, these controllers must identify exactly which of the data processed are subject to the GDPR and to what extent they are able to provide the level of security and protection of the IT system, data integrity and confidentiality of personal data.

There are a number of technologies that practically open the future to new possibilities for data processing, for new kinds of *knowledge* extracted from simple, but enormously collected computer data.

3. Legal threats and safeguards for security and privacy of devices and data

The advancement of technology undeniably presents a range of much-needed advantages that allow for the computerisation and automation of most data processing processes and even real-time self-checking maintenance.

The same advancement of technology and extremely easy access to information is encouraging more and more people to explore the criminal side of the digital age, encouraged by the fact that there are more and more ‘tutorials’ showing how to exploit vulnerabilities of various systems and, moreover, there are malware resource sites that allow a person to initiate a cyber attack without even average computer skills.

Faced with the new challenges and threats, legislators in European countries had to develop a common standard for protecting information systems against different types of attacks through the common assumption of criminalisation of these criminal acts committed against a computer system or using a computer system, and these standards were implemented in national legislation. In the case of Romania, they had their place in special laws, and after the transition to the current Criminal Code on 1 February 2014, they found their natural place in the organic criminal law.

Some of these systems are not essential – if the personal assistant makes

an unnecessary appointment, it is a trivial effort to cancel it. If the home automation system doesn't hit the right temperature, it's an acceptable inconvenience to make manual adjustments to match the environment. If the facial recognition system misfires and allows a criminal to pay to use your identity so that the bank authorises payments ordered by the criminal, it is a considerable inconvenience to resort to the legal protection mechanisms that the bank offers. If in a state of alert and emergency law enforcement will use autonomous drones that are not remotely controlled by human factors and that can decide²³ on their own when a person poses a threat to make use of the non-lethal weapons of peace or lethal weapons of war on hand, it becomes a matter of life and death if that drone makes the wrong decision and authorizes by its own decisions the use of firearms.

On the other hand, thanks to the computerisation of almost all sectors of the economy, every simple gesture we make in our daily routine generates enormous amounts of computer data, the value of which is determined by the organisation interested in buying it on the free market for personal data. Once in the hands of a marketer, this data can be used to target advertising messages to a specific category of consumers or even automatically to users who meet certain pre-defined conditions.

Such a practice may seem innocent, as most people are willing to give their personal data to any merchant offering a pen and a discount promotion. However, at this point in time, when social networks know worrying amounts of personal information about each of their users, this allows them to treat users differently, using algorithms that decide which content appears higher up, directly accessible and which content becomes hidden, perhaps even invisible.

Depending on the intentions of the buyer of this personal data, it can create the illusion of a bubble of like-minded friends or pave the way for 'fake news' disinformation campaigns with devastating consequences from the economy to the exercise of democratic rights. Information is power, and the will of the wielder dictates data processing.

This is the context in which we now find ourselves surrounded by 'smart' devices that make our lives easier, but to an appreciable extent make us dependent on access to these information systems.

In a computerised and ultra-connected democratic society, there is a need for state criminal legal protection against attacks on information systems and the unlawful processing of personal data.

Devices in IoT ecosystems are essentially systems that possess the ability to adapt to user preferences and behaviour, and this can be achieved by collecting an incredibly large amount of personal data of different natures on which they perform statistical and data mining processing to learn and subsequently intuit the needs of the end user.

²³ See Yaacoub J. P., Noura H., Salman O., Chehab A., *Security analysis of drones systems: Attacks, limitations and recommendations, in the Internet of Things*, Elsevier Public Health Emergency Collection, 11:100218, September 2020.

For example, a simple fitness bracelet has a large number of sensors that can record geolocation data such as GPS coordinates, the routes the wearer usually takes in a day, health data such as pulse, heart rate, sleep quality, blood pressure.

It is now publicly recommended by the competent authorities that any company, regardless of its size, should develop and adapt a set of²⁴ cybersecurity policies and procedures to protect both critical business data and any sensitive data, as their effectiveness has been proven, especially since an overwhelming percentage of security breaches could²⁵ be avoided.

Devices that are part of an IoT Ecosystems are devices that present an additional vulnerability precisely because of the ‘link’ they constantly have with the Internet network, practically providing an always open gateway to receive legitimate commands, but at the same time also presenting an additional risk, providing a ‘bridge’ of connection between people with illicit intentions, having their identity protected by the anonymity that the Internet offers, who may try to use this communication channel to make an illicit connection to this device that allows them to access computer data stored on this device.

From a criminal law perspective, the protection offered by the legislator is primarily to criminalise illegal access to a computer system, as a subsidiary offence often in order to commit other offences once in control of the computer system.

The majority of attacks against information systems in the Internet of Things ecosystems target this personal data, due to the fact that – as we have previously pointed out²⁶ – by their very nature these systems collect huge volumes of computer data, most of which is personal to the extent that it is correlated with other information. This information is collected from even the most mundane video surveillance systems which are now priced to allow any home user to be able to remotely video watch their own property, raising new challenges about how this data can be legally used.

This is the main argument that illegal access crimes directed against a smart device not only exist, but are increasing in frequency, as shown by various reports by IOCTA, SOCTA, CERT-RO and similar bodies, without questioning the ethical²⁷ elements of the attackers.

It is also a topical issue who should be responsible for preventing such

²⁴ See Online Trust Alliance – IoT Security & Privacy Trust Framework v2.5, Internet Society, 2017.

²⁵ See Online Trust Alliance - 2018 Cyber Incident & Breach Trends Report. Review and Analysis of 2018 Cyber Incidents and Key Trends to Address, 9 July 2019.

²⁶ See T. Ban, *Current Standards for Information Security and Privacy*, in Nina Gumzej, Olga Sovova (eds.), *Recent Debates in Cyberspace and Artificial Intelligence Law*, ADJURIS International Academic Publisher, Bucharest · Paris · Calgary, 2023, p. 53-71, <https://adjuris.ro/reviste/rdca/Recent%20debates%20in%20cyberspace%20and%20artificial%20intelligence%20law.pdf>.

²⁷ See X. Moldovan, *Towards a new digital ethic*, in Romanian Journal for Personal Data Protection, No. 1, Universul Juridic Publishing House, 2020, pp. 114–119.

cybercrime – a first option would be to hold the owners of the IT systems and communication networks responsible, and in case of non-compliance we should rely on compliance control bodies with administrative sanctions. A second way is for the judiciary to be given the power to respond proportionately²⁸ to the seriousness of the crime in the hope of reducing the prevalence of these crimes, which has so far been achieved to a questionable extent.

Of course, in practice the answer is unanimous that a comprehensive approach to preventing cyber-attacks must be taken both through continued concern for the implementation of security policies and procedures on the part of organisations or end users of legally protected devices and systems due to the extremely dangerous nature if used for illicit purposes.

The advantages offered by technology and the accessibility with which an individual user can start using these new services without prior training often neglects the aspect of educating²⁹ users about online safety issues and the protective measures they can take³⁰ to secure their computer network and increase confidence in the privacy of their personal data. Even small and medium-sized entrepreneurs cannot neglect the need to secure the IT systems they own, and there are explicit recommendations including government³¹ recommendations to this effect.

It must become clear that any user who connects to technology and services offered online, whether this is in the context of carrying out work tasks or in their private life, can always become a target of cyber-attacks³² or online fraud, sooner or later.

Fortunately, the European Union has an active policy to increase its defences against these cyber attacks, developing a strategy³³ which has among its main objectives the protection of critical sectors which now includes the 5G mobile communications and network segment and the interconnected Internet of

²⁸ See A. Cobuz Băgnaru, *The indissoluble link between the need to protect personal data and resistance to cybercrime*, in Romanian Journal for the Protection of Personal Data, No. 1, Universul Juridic Publishing House, 2020, pp. 100–105.

²⁹ See Cybersecurity Framework Platform by the National Institute of Science and Technology (NIST) USA available at <https://www.nist.gov/cyberframework>.

³⁰ See E. Kritzinger, S. Solms, *Cyber Security for home users: A new way of protection through awareness enforcement*, November 2010, in Computers & Security 29(8), p. 840, 847, available via ResearchGate at https://www.researchgate.net/publication/222706832_Cyber_security_for_home_users_A_new_way_of_protection_through_awareness_enforcement.

³¹ See the Cyber Security Planning Guide produced by the U.S. Government, Federal Commission for Commerce (FCC), with input from the Department of Homeland Security, the National Cyber Security Alliance and The Chamber of Commerce, available at <https://www.fcc.gov/sites/default/files/cyberplanner.pdf>.

³² See B. Obotivere, A. Nwaezeigwe, *Cyber Security Threats on the Internet and Possible Solutions*, September 2020 in International Journal of Advanced Research in Computer and Communication Engineering, Vol. 9, Issue 9, 2020, available via ResearchGate at https://www.researchgate.net/publication/346861524_Cyber_Security_Threats_on_the_Internet_and_Possible_Solutions.

³³ See The EU Cybersecurity Strategy for the Digital Decade, December 2020, available at <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>.

Things devices³⁴.

The European Union has succeeded through the drastic reform imposed by Regulation (EU) 2016/679 GDPR and respectively the NIS and NIS2 Directive (soon to be implemented in Romanian law by October 2024 at the latest) to impose much more stringent rules on the ways in which personal data controllers will be able to continue processing personal data, being mandatory to provide a set of safeguards to respect the rights of data subjects.

4. Lessons learned

Even if we hypothetically accept that it is a technology that brings security breaches into our own lives and economic activity, foregoing these benefits is not the solution. There have also been opinions that have considered whether we are safer using computer systems that are not connected to absolutely any form of network or form of communication with other computer systems, in the hope that physical security measures might be sufficient to stop attackers.

Analysing existing studies and recommendations, two general but perfectly valid conclusions can be drawn in the context of cyber safety and security:

The first conclusion is that technology and information systems, interconnected devices and the global network of interconnected sensors offer both fantastic opportunities, but at the same time the threats are real.

The European Union, as the general guarantor of cybersecurity and privacy of personal data, is constantly monitoring new threats and contributing with increasingly specific legislation.

On 22 March 2021 the European Union adopted conclusions³⁵ on the cyber security strategy. *Building a resilient, green and digital Europe* is confirmed as a key strategic objective.

The aim is³⁶ to reduce the number of security breaches while increasing resilience to cyber attacks. It is already not only proven, but accepted and assumed that in the near future the number of cyber attacks will increase dramatically, that they will be difficult to stop, almost impossible to detect at times and can have extremely serious consequences.

The second conclusion is that educating, empowering and encouraging individual and small- and medium-sized corporate users about the measures they can implement and creating a corporate culture of attack prevention is the most

³⁴ See Outcome of Proceedings Council conclusions on cyber security of connected devices, Council of the European Union, December 2020, available at <https://www.consilium.europa.eu/ro/press/press-releases/2020/12/02/cybersecurity-of-connected-devices-council-adopts-conclusions/>.

³⁵ See Council conclusions on EU Cybersecurity Strategy for the Digital Decade, Council of the European Union, available at <https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf>.

³⁶ See Challenges to effective EU cybersecurity policy, briefing report by the European Court of Auditors, March 2019, available at https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf.

effective way to achieve quick but highly effective results.

So, the European Union, through its specialised agencies, has started an aggressive information and education campaign by urging people to act (call to action campaigns) but also by providing highly detailed and accessible guides to help the average user take the first essential steps towards securing their computer networks and the interconnected information systems and devices in the Internet of Things ecosystem.

This responsibility for the security of their own IT networks is, however, also laid down in the main EU Directives and Regulations (e.g. NIS, NIS2, GDPR and others). Now users are taught concrete and WHAT they can do to understand the threats and HOW to take the necessary action.

Open access to official, verified and secure information through official guidelines covers all new technologies such as the Internet of Things³⁷ ecosystems and interconnected³⁸ devices, recommendations on³⁹ cybersecurity challenges, concrete practical recommendations⁴⁰ for securing⁴¹ the Internet of Things devices respecting the Privacy by Design principle, cybersecurity recommendations for the⁴² Internet of Things devices market to reduce the risks of supply chain attacks.

There are a number of tools to prevent cyber-attacks on devices in the Internet of Things ecosystems, broadly grouped under the category of reasonable security measures⁴³, which are extra important now especially in the current increasingly context of home and office automation, both virtual and physical.

The notion of a ‘reasonable’ level of security is a concept that recent European directives bring to the fore. The standard to which the European legislator is moving is that of a ‘reasonable’ level and not that of the highest theoretical level of security, which becomes excessive both in terms of the actual methods of implementation⁴⁴. And in terms of cost, given the specific size of an organisation, the volume of personal data collected and processed and the harmonisation

³⁷ See Baseline Security Recommendations for IoT, ENISA, November 2017, report available at <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot>.

³⁸ See IoT Security Standards Gap Analysis, ENISA, January 2019, report available at <https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis>.

³⁹ See Industry 4.0 – Cybersecurity Challenges and Recommendations, ENISA, May 2019, report available at <https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis>.

⁴⁰ See Good Practices for Security of IoT – Secure Software Development Cycle, ENISA, November 2019, report available at <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1-2>.

⁴¹ See Guidelines for Securing the Internet of Things, ENISA, November 2020, report available at <https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things>.

⁴² See EU Cybersecurity Market Analysis – IoT in Distribution Grid, ENISA, April 2022, available at <https://www.enisa.europa.eu/publications/eu-cybersecurity-market-analysis-iot-in-distribution-grid-2>.

⁴³ See also the NIS Directive (EU 2016/1148) which defines risk as any *reasonably identifiable* circumstance in Article 4(9).

⁴⁴ See EU Directive 2016/679 General Data Protection Regulation which imposes ‘reasonableness’

with other data protection methods provided for by the European legislator such as anonymisation, pseudonymisation, encryption.

The role of reasonable security measures is especially important given that some devices in the Internet of Things ecosystems are purchased expressly to control other devices, based on a ‘trust⁴⁵’ relationship between devices that the user establishes.

A very relevant example of this is voice-activated ‘personal assistant’ devices, connected both to the internet and via ‘trusted⁴⁶’ relationships to other devices such as thermostats, smoke sensors, water sensors, window intrusion sensors, ventilation systems, external window blinds actuation systems and even home alarm systems and remote control of ‘smart’ central locking systems for external building access doors.

Compromising these types of devices will allow an attacker a default control relationship over all other devices in a ‘trusted’ relationship with the compromised personal assistant device, such as Google Home, Amazon Alexa, Apple Homepod and others.

Unfortunately, the reality is that simply educating and bringing to the public’s attention the problems that can arise in the case of unsecured networks or computing devices, non-compliance with the standards required by the GDPR for personal data processing is not enough.

A punitive state repressive component is also absolutely necessary as a response to culpable or bad faith failure to comply with these minimum standards.

On the one hand, making people accountable in terms of fines and administration is a first course of action. Under the regulations of Regulation (EU) 2016/679 GDPR and the NIS and NIS Directive², governmental and union-level entities are established that have the exact powers to control and sanction contravention and administrative offenders.

At the same time, accountability can also be achieved by criminalising certain activities, and it should be noted that even the mere possession of malicious software for the purpose of committing some of the offences provided for by criminal law against information systems is criminal.

Since crimes committed through computer systems can transcend geographical boundaries, an attacker can compromise a computer system remotely without having to be physically present in the vicinity.

For this reason, offences committed through or on computer systems are

as a standard for security measures to be taken to ensure data security, for time limits within which a controller must respond or disputes must be resolved, for a number of fees charged to respond to manifestly unfounded or excessive requests.

⁴⁵ See V. Engen, J. B. Pickering, P. Walland, *Machine Agency in Human Machine Networks. Impacts and Trust implications*, in Human Computer Interaction Novel User Experiences, 18th International Conference, HCI International, 2016, Toronto, Canada, Proceedings, p. 103.

⁴⁶ See Y. Liao, J. Vitak, P. Kumar, M. Zimmer, K. Kritikos, *Understanding the Role of Privacy and Trust in Intelligent Personal Assistant Adoption*, in Proceedings of the 13th Annual iConference, Lecture Notes in Computer Science, vol. 11,420, pp. 102-113.

most often criminal offences that have elements of foreignness and pose significant problems in terms of spatial application of criminal law and the practical establishment of effective jurisdiction.

In practice, this aspect is essential because it provides a concrete answer to the question of *which legal system should be applied in a specific situation*, which is essential when we have to relate the objective and subjective typicality in order to determine whether the act constitutes a crime, what is the legal framework of this act and, of course, from there, the concrete conditions of the application of the various institutions of substantive criminal law and criminal procedural law.

The solution is, of course, easy to see, interstate cooperation in criminal cases to stop cross-border crime, simplifying procedures with foreign elements, especially between EU Member States. Fortunately, these steps are already being taken and the legislative framework is increasingly adapted to the specific needs of investigations.

Bibliography

1. Ban, T., *Current Standards for Information Security and Privacy*, in Nina Gumzej, Olga Sovova (eds.), *Recent Debates in Cyberspace and Artificial Intelligence Law*, ADJURIS International Academic Publisher, Bucharest · Paris · Calgary, 2023, p. 53-71, <https://adjuris.ro/reviste/rdca/Recent%20debates%20in%20cyberspace%20and%20artificial%20intelligence%20law.pdf>.
2. Ban, T., *Fraud committed through information systems and electronic means of payment – Legislative challenges of the digital age*, in Preventing and Combating Cybercrime. The International Conference, Accent Publishing House, Cluj Napoca, 2016, pp. 264–274.
3. Ban, T., *The digital future of law between the opportunities of the cyber era and the acute need for security*, in Curierul Judiciar, no. 6, 2020, pp. 339–345.
4. Ciurea, A., *The Digital Age and Justice (I). Objectives, algorithm design methods and consequences of their use in justice*, in Revista Universul Juridic, No. 1 January 2022, pp. 56–70, available at http://revista.universuljuridic.ro/wp-content/uploads/2022/03/06_Revista_Universul_Juridic_nr_1-2022_PAGINAT_B_T_A_Ciurea.pdf.
5. Cobuz Băgnaru, A., *The indissoluble link between the need to protect personal data and resistance to cybercrime*, in Romanian Journal for the Protection of Personal Data, No. 1, Universul Juridic Publishing House, 2020, pp. 100–105.
6. Dănișor, M. C., *The Rule of Law – Guaranteeing Privacy in the Cyber Era*, in the Rule of Law in the Digital Era. The International Conference, Accent Publishing House, Cluj Napoca, 2016, pp. 118–136.
7. Engen, V., J. B. Pickering & P. Walland, *Machine Agency in Human Machine Networks. Impacts and Trust implications*, in Human Computer Interaction Novel User Experiences, 18th International Conference, HCI International, 2016, Toronto, Canada, Proceedings.
8. Ionita, G. I., *Cybercrime offences. Incriminating, investigating, preventing and combating*, 3rd edition, Universul Juridic Publishing House, Bucharest, 2018.

9. Kritzinger, E. & S. Solms, *Cyber Security for home users: A new way of protection through awareness enforcement*, November 2010, in *Computers & Security* 29(8), pp. 840-847, available via ResearchGate at https://www.researchgate.net/publication/222706832_Cyber_security_for_home_users_A_new_way_of_protection_through_awareness_enforcement.
10. Liao, Y., J. Vitak, P. Kumar, M. Zimmer & K. Kritikos, *Understanding the Role of Privacy and Trust in Intelligent Personal Assistant Adoption*, in *Proceedings of the 13th Annual iConference*, Lecture Notes in Computer Science, vol. 11, 420, pp. 102-113.
11. Moise, A. C., *The criminological dimension of crime in cyberspace*, 2nd edition, C. H. Beck, Bucharest, 2020.
12. Moldovan, X., *Towards a new digital ethic*, in *Romanian Journal for Personal Data Protection*, No. 1, Universul Juridic Publishing House, 2020, pp. 114–119.
13. Obotivere, B. & A. Nwaezeigwe, *Cyber Security Threats on the Internet and Possible Solutions*, September 2020 in *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 9, Issue 9, 2020, available via ResearchGate at https://www.researchgate.net/publication/346861524_Cyber_Security_Threats_on_the_Internet_and_Possible_Solutions.
14. VasIU, I., *Criminalitatea informatică*, Ed. Nemira, Bucharest, 1998.
15. VasIU, I., *Hackers. Cybercriminals or rebels with a cause? (All about hackers)*, Nemira Publishing House, Bucharest, 2001.
16. Voigt, P. & A. Bussche, *The EU General Data Protection Regulation (GDPR). A practical guide*, Springer International Publishing, 2017.
17. Yaacoub, J. P., Noura H., Salman O. & Chehab A., *Security analysis of drones systems: Attacks, limitations and recommendations, in the Internet of Things*, Elsevier Public Health Emergency Collection, 11:100218, September 2020.