International Comparative Jurisprudence 2021 Volume 7 Issue 2
ISSN 2351-6674 (online) DOI: http://dx.doi.org/10.13165/j.icj.2021.12.004

PRIVACY PROTECTION IN THE DIGITAL AGE: A CRIMINAL LAW PERSPECTIVE

Renata Marcinauskaitė
Mykolas Romeris University, Lithuania
E-mail: rennata@mruni.eu

Yulia Razmetaeva
Yaroslav Mudryi National Law University, Ukraine
E-mail: yu.s.razmetaeva@nlu.edu.ua

Received: 25 August 2021; accepted: 22 November 2021
DOI: http://dx.doi.org/10.13165/j.icj.2021.12.004

Abstract. Privacy as a fundamental right faces considerable challenges as people's activities have moved into cyberspace. The development of technology has had an impact on a various areas related to personal privacy. This article discusses changes to the concept of privacy in the digital age, presents approaches to privacy issues in the law of the European Union (EU) and United States (US) today, and reveals the aspects of privacy protection in criminal law based on the relevant Lithuanian case law and Ukrainian law. This analysis showed that legal regulation and practice must be adapted to the changed situation. The use of technology has created new ways of committing serious privacy violations; therefore, criminal law must be ready to properly respond to the changing nature of crimes against personal privacy in the digital age.

Keywords: privacy, inviolability of privacy, digital age, principle of equivalent treatment, EU privacy approach, US privacy approach, Lithuanian privacy approach, Ukrainian privacy approach.

Introduction

The coming of the digital age brought new challenges and perspectives; it influenced all aspects of people's lives, including in the most general sense and in specific modes of action. The features of the digital age can be identified as the following: (1) a significant part of all activities takes place in cyberspace or has an online component; (2) digital tools are extremely common in both public and private life; (3) data has become key to any economic, social, or political activity; (4) the amount of data is large and the speed of its spread is incredibly high; (5) the development of societies is uneven, and this is exacerbated by the digital divide; and (6) the power of business structures is growing, including their ability to modify the behaviour of users of digital tools.

These factors defined crucial changes in attitudes towards human rights and privacy, in particular from a legal perspective. Such changes were not instantaneous, but nor were they imperceptible. From the moment when the development of digital technologies began to gain momentum and penetrate into all spheres of society, serious concerns have been expressed about threats to privacy from such technologies (DeCew, 1997), maintaining privacy in cyberspace (Schwartz, 1999), and dramatic changes in law as such (Hildebrandt, 2015). There are also many concerns about the consequences of the digital age that were not earlier regarded as threats, namely: the indirect impact of digital technologies on democratic societies and the subtle undermining of democratic foundations (Nunziato, 2009; Diamond, 2010; Etling et al., 2010; Liveriero, 2019); changes in the ways and speed we receive information and, accordingly, the perception of media messages by society (Ekstrand, 2015); the disproportionate impact on people and communities that business structures which own digital tools have (Shadmy, 2019); and the impact of the long-lasting digital footprint on human rights and privacy (Rosen, 2012; Ambrose, 2013; Razmetaeva, 2020). The scientific literature also raises questions about the importance of the principle of equivalence in criminal law (Fedosiuk & Marcinauskaitė, 2013), and reveals various privacy concerns in light of developing technologies (Scott-Hayward et al., 2015; Dorraji & Barcys, 2014). At the same time, it

appears that the challenges to privacy posed by the very nature of the digital era are still underestimated, as well as their implications for law, especially for such important and simultaneously conservative areas as criminal law.

This article attempts to address the challenges to privacy that have emerged in the digital age, bearing in mind their impact on criminal law from the points of view of different paradigmatic approaches. For this purpose, a comparative analysis of the EU and US approaches to protecting privacy, its relationship with freedom of expression, and reasonable expectations in the area of privacy in connection with digitalisation is carried out. Conceptual changes in privacy *per se* and their role in defining changes in law, including criminal law, are explored. This article also reveals the significance of the principle of equivalent treatment applied in ensuring the proper interpretation and application of the criminal codes. This principle becomes relevant when actions transgressing the inviolability of privacy are committed in cyberspace. Analysis of case law is used to show the peculiarities of the use of technology and changes in privacy violations, which justify the need for a broad interpretation of private life that applies such concepts to cyberspace.

This paper also turns to the legal answers offered by developed and developing democracies in the area of privacy protection, as exemplified by Lithuania and Ukraine, which rely primarily on a European approach to the interpretation of privacy. The choice of these approaches for comparison is explained by the following reasons: (1) the approaches of the EU and the United States are the most authoritative both from the point of view of influential actors, including the authority of the relevant judicial institutions, and from the point of view of responding legally to the challenges of the development of digital tools; (2) the approaches of Lithuania and Ukraine are taken as those that, in terms of values and regulations, are applied in democratic countries, and at the same time both are based on EU standards; and (3) the comparison of the approaches of Lithuania and Ukraine reflects the different degrees of their compliance with EU standards, and the different strength of democratic institutions and the rule of law in these countries.

The methodology used in this study is interdisciplinary, combining philosophical and practical approaches starting from the anthropocentric idea of human rights and allowing for the justification of the need to take into account changes in privacy so that individuals can maintain control over their lives. The interpretation of different approaches to privacy in this paper is based on an analysis of the case law of the European Court of Human Rights (ECtHR), the Court of Justice of the European Union (CJEU), the Supreme Court of the United States, the practice of the Constitutional Court of the Republic of Lithuania, and the decisions of Lithuanian courts in criminal matters.

1. Changes to the concept of privacy in the digital age

1.1. The essence of these changes

Privacy is one of the broadest fundamental rights, and at the same time a concept that has a significant impact on the lives of individuals and societies in the digital age. The interactions of all subjects of law, which are often mediated today by new communications and digital technologies, include an element of privacy protection, especially in the areas of data protection and online confidentiality. It seems that there have been some changes in the understanding and protection of privacy in the digital age,[1] which are reflected in the following:

(1) Privacy is acquiring the features of a collective phenomenon, where private information can be not only what individuals disclose about themselves, but also what others disclose about them. For example, tagging photos on social media gives basic control over group photo settings to those who upload them. Of course, the person being identified has some tools to stop unwanted data leaks, but these tools may be ineffective or belatedly applied. In addition, public expectations regarding private lives have changed. For instance, such expectations could include the need to have at least one social network account filled with some information. On the one hand, this is a matter of free will, but on the other hand it is a matter of social pressure. Today, we are forced to interact more than ever, even if we do not want to, and to rely on others that control part of our privacy – even if we are not personally acquainted with these others and do not pass on or disclose private information directly to them. Attempts to

[1] Part of this concept was presented at the Data and Ethics: Second Transatlantic Conference, University of Vienna (AUT), Saint Anselm College (USA), University of St. Andrews (UK), Nov 22–23, 2019, Stift Klosterneuburg, Austria. The authors are very grateful to the conference participants for their valuable comments and remarks.

overcome the impact of such interactions include a gradation of privacy, involving recourse to the idea of group privacy. For example, Mariarosaria Taddeo (2020) calls for the need to protect this type of privacy "in the age of big data and artificial intelligence, where data collection is often finalised to identify categories, groups, of individuals rather than to single out a specific person" (p. 173). At the same time, the division of privacy into individual, group, and perhaps the privacy of communities or even societies requires a cautious approach, because it possible to lose the very essence of privacy.

(2) The long-lasting digital footprint is having an increasingly noticeable impact on privacy. A person may forget what private information they have disclosed in the past, or may change their identity, but a lot of information about them is stored for years and can be easily found. In the absence of effective legal (and technical) means of erasing such a trace, reliance remains largely on the fact that individuals will learn to be aware of the consequences of the information about themselves that they leave in the form of data. At the same time, the level of monitoring of the actions of individuals in the digital environment and monitoring by technical means is growing steadily in today's world.

(3) The focus of communication is shifting from people to devices, and private information is increasingly being stored and disseminated through devices. For a long time, privacy was seen in the context of interaction with other people, but today people are increasingly sharing information in contexts other than with live interlocutors. Smartphones are becoming a digital extension of individuals, which may not allow users to properly assess the limits of confidentiality. What people still consider a private conversation is no longer private when it comes to devices. At the same time, these devices, which we unconditionally trust as our digital continuation, constantly interact with each other. The Internet of Things (IoT), defined as "a system of interconnected computing devices with unique identifiers (UIDs) [that] can perform data communications without any human involvement" (Liu et al., 2021, p. 1331), as well as communication between gadgets – when your refrigerator can exchange data with your fitness bracelet, for example – further exacerbate the problem. For example, some researches have shown that with the advent of the IoT, the possibility of using big data as a source of official statistics is increasingly being considered, creating additional ethical and statistical problems (Tam & Kimb, 2018). The accumulation of big data through networks and devices can lead to actual deanonymisation, as confidential user data can be obtained statistically (Vivitsou & Saadatmand, 2016). Therefore, the invasion of privacy becomes possible without the use of personal data due to the connection of different pieces of data and their processing.

(4) A significant part of life, including private life, is moving to the online space. What is rightly called "the massive expansion of the online world" is taking place, and, accordingly, "privacy issues in cyberspace have become a primary concern" (Lee et al., 2020, p. 49). Not everyone chooses to engage online completely voluntarily and knowingly. For example, the COVID-19 pandemic has forced many to turn to Internet interactions. At the same time, the number of people who cannot imagine life without cyberspace, as well as the intensity of the online activity of businesses, organisations, and governments, is steadily growing. The Internet has become such a commonplace and everyday occurrence that it is becoming increasingly difficult to separate online and offline life. Therefore, the question of "How can people feel protected against the threats posed by the Internet when they go online?" (Gosztonyi, 2020, p. 135) is becoming more and more principal.

(5) There is an increasing amount of trust being placed in artificial agents such as AI, as well as in corporations, including the trust of private information to them. First, the digital age gave rise to what Mireille Hildebrandt terms "an artificial world, 'peopled' by myriad of artificial agents" (Hildebrandt, 2015, IX). Invisible algorithms increasingly determine important decisions, including those related to privacy. Meanwhile, the consequences of how defining they are – and, at the same time, their lack of responsibility – have yet to be realised. Second, there is a disproportionate increase in the trust placed in corporations, which are conventionally considered representatives of the private sector of society. In particular, a recent study showed that students displayed a surprising amount of trust in Facebook and Google (Crocco et al., 2020). This is a very disturbing trend, especially as companies "can now access years of past records and link a great variety of data sources, sometimes innocuous on their own but not in the aggregate, to inform an increasingly broad range of decisions" (Williams et al., 2018, p. 79).

It is advisable to consider such changes if we want to apply a consistent concept of privacy in the digital world. In particular, legislation and judicial practice should be based on the fact that it is privacy today that allows

individuals to maintain control over some part of their lives; therefore, balancing rights and legitimate interests must also take into account the shifted yet high importance of privacy. Conservative privacy doctrines cannot provide adequate and effective legal protection any longer, as they lag significantly behind the development of digital tools. At the same time, some of the changes discussed above have already had a significant impact on law in general, defining, among other things, changes in case law, including criminal law.

1.2. Understanding private *and* public

In the digital age, the features of which were mentioned above, the understanding of terms such as *private and public person*, *private and public sphere*, and *private and public interest* should be revised. In particular, the scope of the right to privacy significantly depends on who is the subject of this right – the head of state or its ordinary citizen. However, in today's world, we need to change our attitude to new opinion leaders – digital influencers and popular bloggers, for instance, who often have a more significant influence on us than officials or opposition politicians. Privacy protection regimes depend on the definition of a public person, so – bearing in mind that citizens have the right to know a little more about people making important decisions or shaping our political lives – we should offer an expanded understanding of who we are referring to as a public person.

One could argue that Instagram bloggers, for example, should not be subject to such close attention, because they only entertain an audience, even if it amounts to hundreds of thousands of followers. However, as the well-known case of Princess Caroline of Monaco showed, entertainment also plays a role in the formation of opinions and has a great influence. Further, although the ECtHR has established that the distinction drawn between figures of contemporary society "par excellence" and "relatively" public figures has to be clear, and that protection should be higher in a "secluded place" (*Von Hannover v. Germany*, 2004), in the digital age there are no places truly isolated from any impact, and there is no anonymity that cannot be discovered. In addition, bloggers can express an influential opinion on pressing public issues, call for civil protests, and successfully and irresponsibly advertise someone or something. Therefore, the opportunity to know more about them or to conduct studies that touch on the data of such bloggers can be justified by considerations of public interest.

Given the penetration of digital tools in all spheres of life and the accumulation of overlapping data, one can observe a tendency to establish a complex balance of public and private in online and offline spaces. For instance, we might look to the controversial case *Lopez Ribalda and Others v. Spain* (2018) and consider the issue of the legality of the secret video surveillance of supermarket employees by the manager, who had reasonable suspicions of theft. The court's position contains, among other things, arguments about the different degrees of publicity of the spaces in which the cameras were located, and the expectations of employees regarding the protection of their privacy. In particular, the expectation of the protection of privacy could be very high in places which are private by nature, such as toilets, but it is manifestly lower in places that are visible or accessible to colleagues or to the general public. It should be said that, despite the fact that the ECtHR applies clear criteria of proportionality and generally relies on a dynamic doctrine, in the aforementioned case the three judges came out with a dissenting opinion in which they disagreed about the absence of a violation of privacy. There is no consensus in such cases, even at the EU level, and this is greatly complicated when it turns to the application of law in cyberspace, several jurisdictions, or transnational corporations.

The understanding of private and public may vary in different legal systems. At the same time, regulatory jurisdictions are becoming increasingly interdependent, so a single court decision may affect several states. Another point to consider is the attempt by many governments to apply extraterritorial jurisdiction to issues related to information exchanges, which include threats to privacy. Therefore, potential privacy decisions must be based on specific approaches, among which the approaches used in EU and US law deserve special attention. Being applicable in different jurisdictions, these approaches represent the results of legal thinking and legal practice, which, in turn, influence the decisions made about privacy today.

2. The approaches of EU and US law to privacy issues today

2.1. Differences in approaches to privacy

It appears that the three key differences in the approaches (or legal doctrines) of the EU and the US regarding privacy are as follows:

(1) Miscellaneous balancing of privacy with other rights and interests. Privacy is not an absolute fundamental right, so it needs to be balanced with other human rights as well as legitimate interests. The most frequent conflict situations arise when it comes to the relationship between privacy and freedom of expression. In this regard, the US approach seems to be more protective of free speech, as it is one of the central values of American democracy. In particular, in a complex case regarding the media's publication of a rape victim's name, the US Supreme Court highlighted the sensitivity and importance of the interests represented in the clashes between the First Amendment to the US Constitution and privacy rights, but still ruled that the newspaper was protected by freedom of expression if it "lawfully obtains truthful information about a matter of public significance" (*Florida Star v. B.J.F.*, 1989). Jeffrey Rosen (2012) draws attention to that difference in approaches when he writes about the right to be forgotten and the corresponding privacy issues, emphasising that "Europeans and Americans have diametrically opposed approaches to the problem" (p. 88).

Another type of common conflict is illustrated by the clash of privacy with security interests. As it is fairly noted, "security schemes can contribute to the prevention of privacy infringement. However, preventive security may infringe upon personal privacy" (Lee et al., 2020, p. 51). Here we come to the second significant difference, which is likely due to both the American anti-terrorism legislation, which gives rather broad powers to government agencies, and the role of leading technology corporations in the digital age, many of which arose and operate in American jurisdictions.

(2) Different foci regarding threat. There seems to be a lot of emphasis on privacy protection from government invasions in the EU, while corporations are the main focus in the US. In particular, such differences are visible in the practice of the most authoritative courts of both jurisdictions. For example, such differences are visible in high-profile cases of the ECtHR when it considers direct abuses by the state and offers a test that is necessary when applied to regimes of mass data interception, as in the case of *Big Brother Watch and Others v. the United Kingdom* (2021), or indirect abuses, such as the lack of adequate privacy protection and clarity of law, as in *Benedik v. Slovenia* (2018). The CJEU confirmed that the general and indiscriminate transmission of bulk data is unlawful in *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Other* (2020). In addition, in joint cases C-511/18, C-512/18, and C-520/18, named *La Quadrature du Net and Others* (2020), the CJEU ruled that Article 6 of the EU Charter of Fundamental Rights regarding the right to security "cannot be interpreted as imposing an obligation on public authorities to take specific measures to prevent and punish certain criminal offenses". This Article is a pebble on the scales of privacy, outweighing the interests of national security, at least with regard to massive interception and tracking.

Despite the significant shift that has occurred thanks to the case of *Carpenter v. United States* (2018), when the court ruled that access to records, including the locations of mobile phones, requires a search warrant, a tipping point appears not to have been reached concerning surveillance by technical means and the fact that, in the digital age, it is becoming more and more difficult for people to maintain private space. At the same time, the case of *United States v. Microsoft Corp* (2018) regarding the company's use of cloud data storage and its transfer abroad led to the adoption of new legislation and the expansion of the powers of law enforcement agencies.

(3) Different understandings of reasonable expectations. The understanding of this problem was formed in legal doctrines, and especially in judicial practice, in divergent ways, given the non-identical criteria for measuring justice and the rule of law in the EU and the US. We will dwell on this in a little more detail below.

At the same time, both described approaches seem to be shifting towards a gradual blurring of the distinction between actions performed in physical space and in cyberspace, including privacy violations. First of all, this is expressed in the granting of status to some areas (structures) of cyberspace, analogous to the status of the same spaces (structures) in physical reality. For example, in the case of *Packingham v. North Carolina* (2017), social

media was defined as a "protected space under the First Amendment for lawful speech", that is, it was defined as a place for freedom of expression, a public forum, and not a commercial structure. The fusion of online and offline environments is also expressed in the tightening of requirements regarding the handling of private data, no matter how technically difficult it is to organise it. In particular, in the case of *Orange Romania SA v. The Romanian National Supervisory Authority for the Processing of Personal Data* (2020), the CJEU set out detailed criteria for granting consent to the transfer of data, which must be freely-given, active, and informed. The third aspect, which is especially significant for various types of liability, concerns the infliction of damage in cyberspace, which is closer in both reality and understanding to real damage, including that of an intangible nature. Particularly in the cases of *Spokeo, Inc. v. Robins* (2016) and *TransUnion LLC v. Ramirez* (2021), it was discussed whether actions involving digital data inaccuracies fall under the definition of "concrete harm". Both cases, although not successful for either Robins or Ramirez, respectively, sparked a serious debate about harm. For instance, the Electronic Frontier Foundation's legal brief in support of Ramirez argued that the risks associated with unrestricted data collection by companies have "serious consequences" for many consumers (Brief of Amicus Curiae Electronic Frontier Foundation in support of Respondent, *TransUnion LLC v. Ramirez*, 2021).

This shift is especially important for criminal law, primarily because this means not only the expansion of some legal instruments, such as the addition of electronic evidence to the classical set of evidences of committed crimes, but also doctrinal restructuring, such as the increasing importance of the principle of equivalent treatment.

2.2. Reasonable expectations regarding privacy

The standard of reasonable expectations is an element of the principle of reasonableness, as well as an element of the rule of law and legal certainty. At the same time, in the digital age law is becoming increasingly uncertain, both in view of the lack of norms and principles keeping up with the development of technologies, which could effectively work in digital spheres, and in view of the growing uncertainty as such.

It appears that in US law reasonable expectations regarding privacy are based on criteria applicable to a particular case, and, in this sense, expectations start from the balancing standard. In the concurring opinion in the landmark case *Katz v. United States* (1967), Judge J. Harlan formulated a test of reasonable expectations of privacy, which includes two considerations: an individual must demonstrate an actual expectation of privacy; and the expectation is such that society recognises it as reasonable. However, this undeniably important test, although applied to technology-mediated interventions, primarily concerns the actions of public authorities, whereas in the digital age, such interventions are often carried out by businesses, organisations, and individuals. Remarkably, such interventions are not necessarily related to the criminal intentions of the subjects of law; on the contrary, these subjects may have the best and most conscientious of intentions, but as a result have a negative impact on the protection of privacy and human rights in general. The fact that human habits have changed over the past few years adds to these problems: the growing dependence on digital technology, daily access to social networks and applications, and the widespread use of mobile devices all affect the validity of individual expectations.

In EU law, the concept of reasonable expectations regarding privacy seems to be based on an individual's rights, even if their protection means serious economic losses and prevents unintended technological development. This approach seems to be at the heart of the GDPR, which "protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data" (Regulation of the European Parliament and of the Council 2016/679, 2016). At the level of judicial practice, this approach was once again supported by the impressive decision of the Court of Justice of the European Union, which effectively changed the system of data transmission of EU citizens and confirmed that the protection of certain human rights requires an adequate level of data protection (*Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*, 2020).

It was predicted that the number of devices connected directly to the Internet would rise to become three times the number of people by 2020 (Goad et al., 2021). This indicator not only reminds us once again of the amount of data that is processed upon connection, but also of the issue of control. Who controls these devices and this data? At first glance, it may seem that device owners perform these functions. However, in reality, the levers of control may not be in the hands of individuals at all, which ultimately calls into question control over their own lives and devalues the idea of privacy.

In the digital age, individuals and groups trust a significant share of private data and privacy issues to corporations – whether voluntarily, because they are used to considering their phones and blogs their personal space, or not quite voluntarily, because they are not aware that the "default" privacy settings are designed to collect data. It would be wise if reasonable privacy expectations were based, in the first place, on transparency, responsibility, and confidentiality. However, despite the growing popularity of privacy by design (PbD), in most cases default settings provide free access to a huge amount of data. To ensure that the desired level of privacy is achieved requires significant effort, as those settings are not user friendly at all, and lots of research and alterations need to be made to make one's digital presence safe. Less technologically able people cannot even imagine the risk that they are exposed to. They are also unaware that private information can now be primary, secondary, and even behavioural, and that even their mouse movements are registered. The paradoxical expectations of users regarding the personalisation of services and goods online with the full protection of private data can hardly be called reasonable. At the same time, it seems that most powerful players – corporations, governments, international organisations – support these paradoxical expectations of individuals.

As Luciano Floridi (2016) observed regarding different types of societies and understanding information society, "expectations change contextually" (p. 3). Floridi introduced the characterisation of expectations as indicators that can help gauge the maturity of a society and illustrate when the absence of a societal feature is informative. At the same time, this formula can be applied in a broader context: to the expectations of individuals in the digital age as such. It is worth considering that reasonableness and explicitness of expectations could be connected not only to the level of development of a particular society and the degree of its digitalisation, but also to the cultural layers, values, traditions, and legal doctrines that exist in this society.

Despite attempts by technologically capable professionals to implement legitimate privacy options that also provide users with meaningful privacy control (Feng et al., 2021), these features remain elusive. Privacy is not a set of options that can be turned on and off on a device. This is primarily the value for individuals and the basis for the preservation of today's shrinking living space. In order to ensure the effective legal protection of privacy in the digital era, it is necessary to change the underlying conceptual approach.

3. The protection of privacy in criminal law

3.1. The concept of private life in criminal law

To ensure real, effective protection of the right to privacy, countries reinforce it with both civil and criminal liability for acts of unlawful interference with the private life of an individual. It is important to note in this regard that the case law of the ECtHR warrants an array of legal instruments to ensure respect for privacy, and the nature of the obligation of the state to do so depends on the particular aspect of private life under contention (*Söderman v. Sweden*, 2013). Criminal liability, as *ultima ratio*, is applicable only for the most severe violations of human privacy. The requirement to identify a particular degree of seriousness of the interference with privacy when applying criminal liability pertains to the essence of the *ultima ratio* principle – the "ultima ratio principle has been connected to the relation between criminal law and other less intrusive legislative means" (Melander, 2013, p. 52). Hence, legal regulation to ensure the human right to respect for private life can consist of not only criminal but also of civil remedies; which of the remedies is appropriate and adequate should be decided after the assessment of each specific violation of the right to private life.

The changes in the concept of privacy discussed earlier are also relevant in the area of criminal law. The legal concept of private life in the most general sense is "linked with the state of an individual when the individual may expect privacy, or with legitimate expectations of private life" (Ruling in case No. 12/99-27/99-29/99-1/2000-2/2000, 2000; Ruling No. KT8-N4/2015, 2015). The right to privacy, first of all, seeks to ensure the development of each individual in their relationships with other individuals without external interference. On the other hand, criminal laws do not normally detail the concept of private life; therefore, a decision in criminal cases as to what belongs to the private life of a particular individual and which information is within the scope of private life of a particular individual is based on the assessment of all circumstances identified in the proceedings. Hence, it is noted in the case law of Lithuanian courts that any assessment of such circumstances as a whole needs to take into consideration the relationship of the information collected with the private life of a particular individual: whether it relates to truly sensitive aspects of private life; whether, although not being intimate in itself, it has been

collected in the ways interfering with privacy, which must normally be authorised by the court; or whether it is only more general information, quite often disclosed by the person themselves in different cases (Ruling in criminal case No. 1A-19-300/2019, 2019).

Privacy protection in Ukrainian law is based upon the Constitution of Ukraine (1996), which proclaims the right of everyone to inviolability of home (Article 30), privacy of correspondence, telephone conversations, telegraph and other correspondence (Article 31), as well as the inadmissibility of interference in private (personal and family) life if it is not provided for by the Constitution Ukraine (Article 32). Within the framework of Article 32, everyone is guaranteed the right to become acquainted with information about oneself that is not a state or other secret protected by law, as well as the right to refute false information about oneself and their family members, to demand the removal of such information, and to receive compensation for moral damage caused by the collection, storage, use, and dissemination of such inaccurate information. These articles were clarified in the decisions of the Constitutional Court of Ukraine. It is noteworthy that the Court found the following: "The right to private and family life <...> is considered as the right of an individual to be autonomous independently of the state, local governments, legal entities and individuals" (Ruling No. 2-rp, 2012).

It is also important from the perspective of criminal law that the abovementioned right is established not only in national law but also in international (European Union) legal instruments including, *inter alia*, in Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (Convention), and in Article 7 of the Charter of Fundamental Rights of the European Union (Charter). It is clear that this legal category, although it does not lend itself to strict classification, should be described as broadly as possible in criminal law. In addition, the aforementioned Convention, in particular Article 8 thereof, equally serves as the foundation for the protection of the right to privacy in Ukraine. This is possible since the Convention has been ratified and implemented into the legal system of Ukraine as a directly applicable legislation, having priority in legal force over the laws of Ukraine.

Article 8 of the Convention, which lays down the right to the respect for private and family life, states that "everyone has the right to respect for his private and family life, his home and his correspondence". The provision on private and family life is also similarly worded in Article 7 of the Charter: "everyone has the right to respect for his or her private and family life, home and communications". These categories of privacy are also mentioned in the jurisprudence of the Constitutional Court of the Republic of Lithuania:

> "The Constitution provides that the private life of a human being is the personal life of an individual: the way of life, marital status, living surroundings, relations with other people, views, convictions, habits of the individual, his physical and psychological state, health, honour, dignity, etc. The inviolability of the private life of a human as established in Article 22 of the Constitution presupposes the right of a person to privacy. The right of a human being to privacy encompasses the inviolability of private, family and house life, physical and psychological inviolability of a person, secrecy of personal facts and a prohibition on publicising received or collected confidential information etc." (Rulings in Cases No. 14/98, 1999; No. 12/99-27/99-29/99-1/2000-2/2000, 2000; No. 34/2000-28/01, 2002; No. 3/01, 2003).

It follows from this jurisprudence that a guarantee of the inviolability of private life should also be regarded as one of the elements of the constitutional protection of human dignity: "Arbitrary and unlawful interference with the private life of an individual also means an assault against his (her) honor and dignity" (Ruling in Case No. 14/98, 1999).

It has been noted above that it is impossible to provide an exhaustive definition of private life and set its clear limits (*inter alia*, in criminal law); therefore, the status of particular data will depend on the context of a large number of circumstances at issue. It should, however, be noted that such a necessity does not exist in fact – as was pointed out by the ECtHR in the case *Niemietz v. Germany*. The Court noted in its judgment that

> "[t]he Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of "private life". However, it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world

> not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings" (*Niemietz v. Germany*, 1992).

Although, as mentioned, an exhaustive definition of the area of personal privacy is actually impossible, its outline and internal structure, although in abstract terms, can, nevertheless, be defined with reference to the very description of the right to privacy provided in international and national legal acts and from its interpretations in the jurisprudence. Hence, mutually interrelated areas of personal independence can comprise, for example, private and family life, home and personal correspondence, or territorial, information, and communication privacy as relevant from the perspective dealt with in this article. Although such categorisations are of a more theoretical, methodological nature, they are helpful for a clearer understanding of the internal structure of the system chosen in criminal laws for criminal offences violating the private life of an individual.

For example, Chapter XXIV of the Criminal Code of the Republic of Lithuania (CC) sets out crimes against the inviolability of a person's private life. Violations of territorial privacy are criminalised in Article 165 of the CC, which provides for liability for unlawful intrusion into a person's dwelling; liability for communication privacy is established in Article 166 of the CC, which describes the elements of a violation of the inviolability of a person's correspondence; and privacy violations relating to the unlawful possession of information about the private life of another person are set out in Articles 167 and 168 of the CC. These articles define the unlawful collection of information about a person's private life, as well as the unlawful disclosure or use of such information. Similar criminal offences relating to violations of these areas of privacy can also be seen in the criminal laws of the Republic of Estonia and the Republic of Latvia. For example, the Estonian Penal Code (2002), *inter alia*, sets out the following criminal acts relevant in the aspect under consideration: violation of the confidentiality of messages (paragraph 156); illegal disclosure of personal data (paragraph 157); illegal disclosure of specific categories of personal data or data concerning the commission of an offence or falling victim to an offence (paragraph 1571); and illegal use of another person's identity (paragraph 1572). The Latvian Criminal Code (1999), *inter alia*, establishes criminal liability for violating the confidentiality of correspondence and information to be transmitted over telecommunications networks (Section 144) and illegal activities involving the personal data of natural persons (Section 145). These criminal offences are treated as criminal offences against the fundamental rights and freedoms of a person (Chapter XIV).

Regulatory guarantees for the protection of privacy are specified in special legislation, primarily in the Law of Ukraine "On Personal Data Protection" (2010). In particular, it is interesting that this law contains a rather vague wording of private data, which may be classified as confidential information about a person by law or by the person concerned (Article 5). In addition, there are elements of privacy protection in sectoral legislation. In particular, the Criminal Code of Ukraine (2001) criminalises: violation of privacy (Article 182); violation of the inviolability of the home (Article 163); violation of the secrecy of correspondence, telephone conversations, telegraph, or other correspondence transmitted by means of communication or through a computer (Article 164); and theft, misappropriation, and extortion of documents (including private ones), stamps, and seals, their acquisition by fraud or abuse of office, or their damage (Article 357).

In order to qualify the criminal offences relating to privacy violations in a proper manner, it is important not only to understand that a person's private life is a broad category which does not lend itself to a precise definition in all cases, but also to understand that the right to the respect of private life must be interpreted dynamically, taking into account, *inter alia*, societal developments, as well as scientific and technological progress, which provides further possibilities for interfering into the private life of a person (Ruling No. KT13-N5/2019, 2019). In criminal law, these aspects can raise the question as to whether the elements of criminal offences established in criminal laws can, with technological developments, be applied when qualifying private life violations committed in cyberspace. This question, *inter alia*, relates to the specifics of cybercrime – the "move" of traditional crimes against privacy into cyberspace has changed the possibilities for their commission: they have acquired particular specifics according to communication possibilities in cyberspace as well as major differences from the criminal offences committed in the physical space. In order to find an answer to this question, the principle of equivalent treatment becomes relevant (Fedosiuk & Marcinauskaitė, 2013, p. 12).

The scientific literature notes that

> "[t]he evaluative principle of equivalent treatment in physical and cyberspace basically reflects the idea that legal provisions should provide equal requirements for the actions, performed both in physical and cyberspace. In the field of Criminal Law it would mean that an equal assurance of values in both of these spaces is provided through equal evaluation of criminal conducts committed in physical and cyber spaces" (Fedosiuk & Marcinauskaitė, 2013, p. 12).

The requirements of this principle are also reflected in the case law of Lithuanian courts in criminal cases concerning personal privacy; the interpretation provided in the case law makes privacy considerations also admissible in the context of cyberspace. For example, the Supreme Court of Lithuania held in the Ruling of 6 January 2015 in criminal case No. 2K-138/2015 that the offender, *inter alia*, had illegally accessed the victim's e-mail account and copied their private correspondence. Later, the offender sent such information collected in a criminal manner about the victim's private life to other persons via different e-mail addresses. The court of the cassation instance qualified such a criminal offence under Article 168 of the CC, i.e., as the public disclosure of unlawfully collected information about the private life of a person without the person's consent. It was noted in this criminal case that:

> "<...> first of all, <...> Article 168 of the CC criminalises not only private life violations in physical but also in cyberspace. <...> The provision laid down in Article 168(1) of the CC <...> regulates the privacy violation instances, which have been specifically distinguished by the legislator. Secondly, it is also important that public disclosure of information about another person's life can take place not only in physical but also cyberspace, therefore, the information made public on this space (e.g., by e-mail) has all the attributes of electronic data."

Such an interpretation offers an insight into an important aspect of the qualification of privacy violations in both physical and cyber spaces: irrespective of the space (physical or cyber) in which personal privacy is attacked, the same article of the criminal law can be applied to such offences. Such an approach also allows for the same protection of privacy in both spaces to be ensured. To be able to apply such an interpretation, it is necessary to use technology-neutral terms in the descriptions of criminal offences against personal privacy in criminal laws.

3.2. Relevant aspects of the violation of a person's private life using new technologies in Lithuanian and Ukrainian case law

With the development of various technologies, some information about personal, family, and home life has moved into cyberspace. Such a process can be viewed as natural as "[g]iven the extreme influx of technology in our society, it has become almost impossible to avoid its regular utilization" (Sisk, 2016, p. 119). On the other hand, considering the threats to privacy resulting from the opportunities opened by technologies, "[t]hese emerging technologies have forced us to ask a very important question: Is technology destroying our precious privacy?" (Dorraji & Barcys, 2014, p. 309). It is relevant in this regard to consider an overview of the case law of Lithuanian courts in criminal cases relating to personal privacy violations, and to assess how privacy violations are expressed when offenders make use of new technologies. The problems of the interpretation and application of the CC when criminal offenses are committed in cyberspace are also relevant.

At the same time, despite an impressive legal framework, the protection of privacy in the digital age in Ukraine seems to have remained rather ineffective, as evidenced by the lack of court cases at the Supreme Court level that address pressing issues of digital aspects of privacy, as well as relevant ECtHR decisions. Although the ECtHR has made quite a few decisions regarding Ukraine, and some of them concern privacy, a significant part of these cases has focused on the traditional aspects of privacy protection. For example, in the context of criminal law, these decisions were devoted to disproportionate interference in the secrecy of the paper correspondence of persons deprived of their liberty and serving sentences (*Belyaev and Digtyar v. Ukraine*, 2012); and in the context of protecting private data, they related to insufficient protection of sensitive information about the mental illnesses of persons (*Panteleyenko v. Ukraine*, 2006; *Zaichenko v. Ukraine (No. 2)*, 2015; *Surikov v. Ukraine*, 2017). Since the ECtHR does not go beyond its competence, considering the applications filed against the states parties to the

Convention by representatives of these states, it seems that the absence of cases on digital aspects of privacy may mean the absence of Ukrainian requests.

Attempts to solve the problem of the protection of privacy in the digital age have been made in recent years, however, the main method remains the introduction of rather formal changes in Ukrainian legislative acts without the development of appropriate judicial practice. A factor that will possibly contribute to the improvement of the situation may be the convergence of the legal framework of Ukraine and its harmonisation with EU legislation, primarily due to the Association Agreement between the European Union and the European Atomic Energy Community and their member states, of the one part, and Ukraine, of the other part, signed in 2014.

Unauthorised access to the information stored in information registers. It should be noted that "[t]echnology was a primary factor in the rise of information collection" (Solove, 2004, p. 14). Technologies are used by state authorities to compile and systematise information, which, *inter alia*, can fall within the scope of personal privacy, in information registers, or in relevant information systems. It should be underlined in this regard that the fact in itself that information is already in the public domain does not necessarily exclude the protection available under Article 8 of the Convention. Even public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities; this is all the more true where the information concerns a person's distant past – for example, their criminal record (*M. M. v. the United Kingdom*, 2012). Personal data relating to the most intimate and personal aspects of an individual, such as health status, ethnic or racial origin, or criminal record, constitute particular elements of private life falling within the scope of the protection of Article 8 of the Convention. The protection of such data against any misuse is highly important (*Magyar Helsinki Bizottság v. Hungary*, 2016; *S. and Marper v. the United Kingdom*, 2008; *E.B. and others v. Austria*, 2013). The main problem in applying criminal responsibility in such cases is the relation between the abuse of office (Article 228 of the CC) and breaches of privacy. The purpose of criminalising the abuse of office is to ensure the normal, efficient, and lawful activities of institutions or persons with administrative powers or providing public services (Criminal Case No. 2K-87-942/2017, 2017). Such institutions also include the police. It should be noted that the fact that electronic data are officially collected and stored in public registers does not deny responsibility not only for abuse of office, but also for violations of privacy.

There have been cases in the case law of Lithuanian courts where they have identified misuse of access to information registers and other information systems where a large quantity of information, *inter alia*, relating to personal data, is held. For example, it was held in one criminal case that a police officer who had been authorised to work with information registers in the information system of the police collected data about the private life of a large number of individuals and later handed over such data to another person. The court held in this case that the police officer not only abused their official position, but also violated the right of the above-referred-to persons to privacy:

> "<...> The actions of A. A. and M. S. were not one-off or accidental, they had continued for a rather long time; as unlawfully requested by V. R., information had been collected about the life of a large number – 34 persons, this information concerned various private life aspects of the persons, it had been obtained using a large number of different information resources (VRIS CDB, AUDIT III information system, POLIS II browser), part the data collected had been illegally used for the benefit of private detective V. R., thereby causing damage to the victims. <...> the victims questioned during the trial confirmed that they had suffered both material and non-material damage as a result of the criminal acts of the convicted persons: after becoming aware that information had been illegally collected about their private life, they felt disquiet, suffered psychological problems, the feeling of insecurity because the circumstances in which the information collected had been used were unknown, they had fear because of themselves and their close ones" (Criminal Case No. 2K-348-648/2018, 2018).

According to the principle of equivalent treatment, the same CC Articles that criminalise violations of privacy in physical space were applied in this criminal case: Article 167 of the CC (Unlawful collection of information about a person's private life) and Article 168 of the CC (Unauthorised disclosure or use of information about a person's private life).

Unauthorised access to the content of electronic communications. Technological developments have expanded the possibilities of interpersonal communication through the use of social networks that connect member groups that share certain common interests by means of mobile applications, e-mail, which makes it possible to send and receive letters by means of electronic communication, etc. As a result, personal privacy can be violated through unauthorised access to such resources and, accordingly, to the content of private communications. As mentioned before, the transfer of a person's private life to cyberspace has created problems in the interpretation and application of the CC. More specifically, it has raised the problem of whether existing CC Articles that define crimes against the inviolability of a person's private life can be applied to qualify criminal offences in cyberspace. Noteworthy in this context is the notion that the concept of a person's private life is interpreted broadly to include a person's private life in both spaces – physical and cyberspace. Such a broader interpretation follows from the Lithuanian case law.

An overview of the case law of Lithuanian courts shows that there have been criminal cases where the privacy of personal communication has been violated; for example, through unauthorised access to a Facebook account. In one criminal case, it was identified that an offender

> "<...> had used a laptop <...> and a mobile phone <...> to log into the account of A. K. on www.facebook.com 485 times unlawfully and watch, without any authority, the messages sent by A. K. and her chats on electronic communication networks, follow her friends and see pictures, thereby violating the inviolability of personal correspondence" (Criminal Case No. 1-3799-888/2019, 2019).

In another criminal case, the court found violations of the victim's private life because the offender

> "<...> had logged into the personal account of S. J. on the social network www.facebook.com unlawfully and changed her login data without the consent and knowledge of S. J. by entering his own password for the account of S. J. on Facebook, and thereby unlawfully accessed this account. Without any knowledge and agreement of S. J., he shared personal pictures where she was nude in the section 'Story', used the chat application Messenger that was connected to the profile 'S. J.', watched the content of the information sent by electronic communication networks, correspondence with other persons, wrote messages to other persons on behalf of S. J., sent personal pictures of S. J., read replies, and breached the inviolability of communication of S. J. by such actions" (Criminal Case No. 1632-1091/2021, 2021).

In another criminal case, a violation of the inviolability of communication was found because the offender had accessed the application Tinder:

> "<...> at home <...>, unlawfully and against the will of D. V., [he] took away her mobile phone in the bathroom <...>, went to the bedroom and watched the content of information sent by electronic communication networks, correspondence with other persons on the application Tinder and SMS, and thereby breached the secrecy of the messages sent by technical correspondence devices by the victim" (Criminal Case No. 1-89-373/2021, 2021).

There are many criminal cases in the case law of the Lithuanian courts where the courts identified offenders logging into victims' e-mail accounts unauthorised, which enabled unauthorised access to private e-mails. For example, it was identified in one criminal case that, without permission from the victim, one person

> "<...> had unlawfully used the login name and password known to him, logged into the e-mail account <...>, accessed its settings where he rerouted letters to the e-mail account <...> he was using, and in this way watched the content of information sent by electronic communication networks, correspondence with other persons, and read replies" (Criminal Case No. 1-1569-914/2018, 2018).

The case law shows that it is guided by a broad concept of a person's private life, recognising that the expansion of cyberspace has led to new kinds of serious privacy violations. Private life must be interpreted dynamically, taking into account developing technologies. Such an approach allows for the more flexible interpretation of CC Articles, adapting existing norms to changes that have occurred since many activities "moved" into cyberspace. Therefore, relevant criminal offences such as violations of the inviolability of a person's correspondence, unlawful

collection of information about a person's private life, and unauthorised disclosure or use of information about a person's private life exist not only in the physical space but can also be encountered in cyberspace.

Unlawful collection of information through the use of the Global Positioning System (GPS). The use of technical devices to watch and spy on persons, *inter alia*, by using GPS, which enables tracking the location of a person, can lead to a breach of personal privacy. The scientific literature notes that "[t]oday <...> GPS ubiquitously appears in everyday devices from our cars to smart phones. Importantly, GPS-enabled devices allow their users to be tracked, raising privacy concerns <...>" (Scott-Hayward et al., 2015, p. 33). The Supreme Court of Lithuania (2014) held in this regard that

> "the scope of protection of private life against interference by another private person depends, *inter alia*, on the mutual relations of these persons, which determine the limits of privacy with respect to each other. Systematic collection of information about a person by means of GPS-enabled equipment can limit the person's right to privacy, in particular, where such information is used to exert some influence on the person" (Criminal Case No. 2K-213/2014, 2014).

Such an approach is also upheld by lower instance courts. For example, it was found in one criminal case that

> "R. D. had been illegally collecting information about private life, deliberately installed a location device GPS Tracker <...> inside the car <...> that belonged to his partner, and deliberately, intentionally and with premeditation kept tracking the location of the victim R. Z." (Criminal Case No. 1-741-1000/2018, 2018).

A breach of the inviolability of another person's private life was also found in another criminal case, where an offender

> "<...> attached a GPS Tracker <...> with tracking and listening functions under the rear bumper of the car <...> of his former spouse D. R., which made it possible to track the location of the car and unlawfully collect information about the private life of his former wife D. R. – the movement of her car and her location with the help of the above-referred equipment <...>" (Criminal Case No. 1-1109-729/2018, 2018).

These cases reveal that the use of new technologies forces us to rethink the understanding of a person's private life and recognise the new ways of committing criminal offenses against a person's privacy.

It follows that the positive impact of technologies in expanding the possibilities of personal communication also implies the risks of misuse of such technologies, which lead to violations of the right to privacy. With the changing *modus operandi* of offences against the inviolability of private life in the digital age, criminal law should identify such violations and ensure the protection of personal privacy both in physical spaces and in cyberspace in line with the pace and directions of development of modern technologies. Such an approach should be based on a broad concept of a person's private life, which allows for the proper application of the already existing CC Articles that establish criminal responsibility for crimes against the inviolability of a person's private life.

Conclusions

Legal regulation and law enforcement practices must be adapted to technological changes and must take into account innovative ways of committing serious privacy violations. In addition, it must be understood that there is primary, secondary, and behavioural private information, and complete anonymity and complete control is hardly possible in the digital age. Today, reasonable expectations that privacy can be protected should include revising the concept of privacy and applying effective mechanisms to protect it, using a responsible and ethical approach based on human rights. It is also necessary to take into account changes in the understanding of private and public. A combination of legal instruments should be used that can help protect privacy from interference by governments, businesses, organisations, communities, and individuals. It is advisable to consider all of the above-mentioned as relating to law in general and criminal law in particular.

The EU and US approaches to privacy demonstrate different understandings of the right to private life, its balancing with other fundamental rights and legitimate interests, and different attitudes as to the nature of the key

threats to and the main reasonable expectations regarding privacy in the digital age. At the same time, both approaches are shifting towards a gradual blurring of the distinction between actions in physical space and in cyberspace. The same is true for privacy intrusions.

Effectively ensuring the right to the respect for private life by means of criminal law is, among other things, connected with the proper unfolding of the content of private life while, *inter alia*, bearing in mind that it is impossible to provide an exhaustive definition and identify the scope of private life. Decisions in criminal cases as to whether particular information falls within the scope of the private life of a particular individual are made taking into consideration all the circumstances identified.

As technologies keep developing, the principle of equivalent treatment is relevant for the qualification of criminal offences against the inviolability of private life, which means that the same criminal legal measures must be applied for ensuring the right to privacy (irrespective of where – physical space or cyberspace – a criminal offence has been committed). The analysis of Lithuanian case law demonstrated the importance of such an approach.

The analysis of Lithuanian case law shows that, with the "move" of private life to cyberspace, this space has also become exposed to criminal offences which are committed by taking advantage of the possibilities offered by new technologies. The cases of unauthorised access to the information stored in information registers and to the content of electronic communications, alongside the unlawful gathering of information through the use of GPS, show that criminal law must be ready to respond properly to the changes in the *modus operandi* of crimes against personal privacy. It may not be excluded that the development of new technologies can bring new, unknown aspects pertaining to the use of technologies for intrusion into personal privacy.

The reasons for the low efficiency of privacy protection in the digital age in Ukraine may be regarded as the following: (1) problems with the rule of law and, accordingly, with the real independence of the judiciary; (2) the absence of a strong tradition of respect for privacy stemming from the Soviet past of Ukrainian society; and (3) the general weakness of democratic institutions in Ukraine, including the lack of a strong voice of civil society institutions on privacy issues in a digital context. This highlights the difference between strong and weak democracies in the post-Soviet period in countries such as Lithuania and Ukraine in particular. Both countries, which were under the yoke of the Soviet regime for a long time, have been restoring the values, traditions, and mechanisms of protecting the right to private life; however, Lithuania's path to its effective protection seems to have been more successful thus far.

References

Ambrose, M. L. (2013). It's about time: Privacy, information lifecycles, and the right to be forgotten. *Stanford Technology Law Review*, *16*(2), 369–422.

Brief of Amicus Curiae Electronic Frontier Foundation in support of Respondent, No. 20-297, in TransUnion LLC v. Ramirez, 594 U.S. (2021). Retrieved from https://www.supremecourt.gov/DocketPDF/20/20-297/171461/20210310110521542_FINAL%20TransUnion%20Amicus.pdf

Constitution of Ukraine (1996), edition of 1 January 2020. Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

Crocco, M., Segall, A., Halvorsen, A. L., Stamm, A., & Jacobsen, R. (2020). "It's not like they're selling your data to dangerous people": Internet privacy, teens, and (non-)controversial public issues. *The Journal of Social Studies Research*, *44*(1), 21–33. https://doi.org/10.1016/j.jssr.2019.09.004

DeCew, J. W. (1997). *In pursuit of privacy: Law, ethics, and the rise of technology*. Ithaca, N.Y.: Cornell University Press.

Diamond, L. (2010). Liberation technology. *Journal of Democracy*, *21*(3), 69–83. https://doi.org/10.1353/jod.0.0190

Dorraji, S. E., & Barcys, M. (2014). Privacy in digital age: Dead or alive?! Regarding the new EU data protection regulations. *Social technologies*, *4*(2), 292–305. https://doi.org/10.13165/ST-14-4-2-05

Ekstrand, V. (2015). *Hot news in the age of Big Data: A legal history of the hot news doctrine and implications for the digital age*. Lfb Scholarly Pub Llc.

Etling, B., Faris, R., & Palfrey, J. (2010). Political change in the digital age: The fragility and promise of online organizing. *SAIS Review of International Affairs*, *30*(2), 37–49. Retrieved from https://www.muse.jhu.edu/article/403437

Fedosiuk, O., & Marcinauskaitė, R. (2013). Criminalization of cybercrime and principle of equivalence. *Administratīvā un krimināla justīcija*, *2*(63).

Feng, Y., Yao, Y., & Sadeh, N. (2021). A design space for privacy choices: Towards meaningful privacy control in the Internet of Things. *CHI'21: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, Article No. 64. https://doi.org/10.1145/3411764.3445148

Floridi, L. (2016). Mature information societies – a matter of expectations. *Philosophy & Technology*, *29*, 1–4. https://doi.org/10.1007/s13347-016-0214-6

Goad, D., Collins, A., & Gal, U. (2021). Privacy and the Internet of Things − An experiment in discrete choice. *Information & Management*, *58*(2), 103292. https://doi.org/10.1016/j.im.2020.103292
Gosztonyi, G. (2020). The European Court of Human Rights: Internet access as a means of receiving and imparting information and ideas. *International Comparative Jurisprudence*, *6*(2), 134–140. http://dx.doi.org/10.13165/j.icj.2020.12.003
Hildebrandt, M. (2015). *Smart technologies and the end(s) of law: Novel entanglements of law and technology*. Cheltenham: Edward Elgar Publishing.
Judgement in criminal case No. 1-1569-914/2018, District Court of Šiauliai, 30 November 2018.
Judgement in criminal case No. 1-89-373/2021, District Court of Utena, 31 March 2021.
Judgement of Belyaev and Digtyar v. Ukraine, 16984/04, ECHR 76 (2010).
Judgement of Benedik v. Slovenia 62357/14, ECHR 363 (2018).
Judgement of Big Brother Watch and Others v. the United Kingdom – 58170/13, 62322/14 and 24960/15, ECLI:CE:ECHR:2021:0525JUD005817013, 25 May 2021.
Judgement of Carpenter v. United States, No. 16-402, 585 U.S. (2018).
Judgement of Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems, Case C-311/18, ECLI:EU:C:2020:559, 16 July 2020.
Judgement of E.B. and others v. Austria, Applications No. 31913/07, 38357/07, 48098/07, 48777/07 and 48779/07, ECLI:CE:ECHR:2013:1107JUD003191307, 14 June 2018.
Judgement of Florida Star v. B.J.F., 491 U.S. 524 (1989).
Judgement of Katz v. United States, 389 U.S. 347 (1967).
Judgement of La Quadrature du Net and Others, French Data Network and Others, Ordre des barreaux francophones et germanophone and Others, Grand Chamber, Joined Cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791, 6 October 2020.
Judgement of Lopez Ribalda and Others v. Spain, ECHR 14 (2018).
Judgement of M.M. v. the United Kingdom, Application No. 24029/07, ECLI:CE:ECHR:2012:1113JUD002402907, 13 November 2012.
Judgement of Magyar Helsinki Bizottság v. Hungary, Application No. 18030/11, ECLI:CE:ECHR:2016:1108JUD001803011, 8 November 2016.
Judgement of Niemietz v. Germany, Application No. 13710/88, ECLI:CE:ECHR:2012:1113JUD002402907, 16 December 1992.
Judgement of Orange Romania SA v. The Romanian National Supervisory Authority for the Processing of Personal Data (Romanian DPA), Case C-61/19, ECLI:EU:C:2020:901 (2020).
Judgement of Packingham v. North Carolina, 582 U.S. (2017).
Judgement of Panteleyenko v. Ukraine 11901/02, ECHR 667 (2006).
Judgement of Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others, Grand Chamber, Case C-623/17, ECLI:EU:C:2020:790, 6 October 2020.
Judgement of S. and Marper v. the United Kingdom, Applications No. 30562/04 and 30566/04, ECLI:CE:ECHR:2008:1204JUD003056204, 4 December 2008.
Judgement of Söderman v. Sweden, Application No. 5786/08, ECLI:CE:ECHR:2013:1112JUD000578608, 12 November 2013.
Judgement of Spokeo, Inc. v. Robins, 578 U.S. 330 (2016).
Judgement of Surikov v. Ukraine, 42788/06 (Merits and Just Satisfaction), ECHR 100 (2017).
Judgement of TransUnion LLC v. Ramirez, 594 U.S. (2021).
Judgement of United States v. Microsoft Corp., 584 U.S. (2018).
Judgement of Von Hannover v. Germany, EMLR 379 (2004); 40 EHRR 1 (2005).
Judgement of Zaichenko v. Ukraine (No. 2), 45797/09, ECHR 232 (2015).
Lee, J. K., Chang, Y., Kwon, H.Y., & Kim, B. (2020). Reconciliation of privacy with preventive cybersecurity: The bright internet approach. *Information Systems Frontiers*, *22*, 45–57. https://doi.org/10.1007/s10796-020-09984-5
Liveriero, F. (2019). The social bases of self-respect. Political equality and epistemic injustice. *Phenomenology and Mind*, *16*, 90–101. https://doi.org/10.13128/Phe_Mi-26076
Liu, Y., Zhang, J., & Zhan, J. (2021). Privacy protection for fog computing and the internet of things data based on blockchain. *Cluster Computing*, *24*, 1331–1345. https://doi.org/10.1007/s10586-020-03190-3
Melander, S. (2013). Ultima ratio in European criminal law. *European Criminal Law Review*, 3(1), 45–64. https://doi.org/10.5235/219174413806915441
Nunziato, D. C. (2009). *Virtual freedom: Net neutrality, free speech, and democracy in the internet age*. Stanford University Press.
Penal Order in Criminal Case No. 1-741-1000/2018, District Court of Panevėžys, 17 April 2018.
Penal Order in Criminal Case No. 1-1109-729/2018, District Court of Klaipėda, 20 November 2018.
Penal Order in Criminal Case No. 1-3799-888/2019, District Court of Kaunas, 20 December 2019.
Penal Order in Criminal Case No. 1632-1091/2021, District Court of Kaunas, 5 May 2021.
Razmetaeva, Y. (2020). The right to be forgotten in the European perspective. *TalTech Journal of European Studies*, *10*(1), 58–76. https://doi.org/10.1515/bjes-2020-0004
Regulation of the European Parliament and of the Council 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (2016) and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 1–88.
Rosen, J. (2012). The right to be forgotten. *Stanford Law Review ONLINE*, *64*, 88–92.
Ruling in Case No. 14/98, Constitutional Court of the Republic of Lithuania, 21 October 1999.
Ruling in Case No. 12/99-27/99-29/99-1/2000-2/2000, Constitutional Court of the Republic of Lithuania, 8 May 2000.
Ruling in Case No. 36/2000, Constitutional Court of the Republic of Lithuania, 23 October 2002.
Ruling in Case No. 34/2000-28/01, Constitutional Court of the Republic of Lithuania, 19 September 2002.
Ruling in Case No. 3/01, Constitutional Court of the Republic of Lithuania, 24 March 2003.
Ruling in criminal case No. 2K-213/2014, Supreme Court of Lithuania, 6 May 2014.
Ruling in criminal case No. 2K-138/2015, Supreme Court of Lithuania, 6 January 2015.

Ruling in criminal case No. 2K-87-942/2017, Supreme Court of Lithuania, 13 April 2017.
Ruling in criminal case No. 2K-348-648/2018, Supreme Court of Lithuania, 29 November 2018.
Ruling in criminal case No. 1A-19-300/2019, Šiauliai Regional Court, 22 February 2019.
Ruling No. 2-rp, Constitutional Court of Ukraine, 20 January 2012. Retrieved from https://zakon.rada.gov.ua/laws/show/v002p710-12#n51
Ruling No. KT8-N4/2015, Constitutional Court of the Republic of Lithuania, 26 February 2015.
Ruling No. KT13-N5/2019, Constitutional Court of the Republic of Lithuania, 18 April 2019.
Schwartz, P. (1999). Privacy and democracy in cyberspace. *Vanderbilt Law Review*, *52*, 1610–1701.
Scott-Hayward, C. S., Fradella, H. F., & Fischer, R. G. (2015). Does privacy require secrecy: Societal expectations of privacy in the digital age. *American Journal of Criminal Law*, *43*(1).
Shadmy, T. (2019). The new social contract: Facebook's community and our rights. *Boston University International Law Journal*, *37*, 307–354.
Sisk, E. P. (2016). Technical difficulties: Protecting privacy rights in the digital age. *New England Journal on Criminal and Civil Confinement*, *42*(1).
Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. New York: New York University Press.
Taddeo, M. (2020). The ethical governance of the digital during and after the COVID-19 pandemic. *Minds & Machines*, *30*, 171–176. https://doi.org/10.1007/s11023-020-09528-5
Tam, S. M., & Kimb, J. K. (2018). Big Data ethics and selection-bias: An official statistician's perspective. *Statistical Journal of the IAOS*, *34*(4), 577–588.
The Criminal Code of Ukraine (2001), No. 2341-III, edition of 8 August 2021. Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text
The Estonian Penal Code (2002). Retrieved from https://www.riigiteataja.ee/en/eli/522012015002/consolide
The Latvian Criminal Code (1999). Retrieved from https://www.warnathgroup.com/wp-content/uploads/2015/03/Latvia-Criminal-Code.pdf
The Law of Ukraine No. 2297-VI "On Personal Data Protection", 1 June 2010. Retrieved from https://zakon.rada.gov.ua/laws/show/2297-17#Text
Vivitsou, M., & Saadatmand, M. (2016). *Privacy in the era of big data and learning analytics: Ethical considerations and positions*. In Ethical and Privacy Issues in the Design of Learning Analytics Applications: 2nd Workshop on Ethics & Privacy in Learning Analytics @ LAK1, University of Edinburg, Edinburgh, UK, Learning Analytics Community Exchange LACE.
Williams, B., Brooks, C., & Shmargad, Y. (2018). How algorithms discriminate based on data they lack: Challenges, solutions, and policy implications. *Journal of Information Policy*, 8, 78–115. https://doi.org/10.5325/jinfopoli.8.2018.0078