Sławomir Oliwniak
University of Bialystok

INTERPRETATION OF THE RIGHT TO PRIVACY IN THE 21th CENTURY. INTRODUCTORY REMARKS

"A free society should not have to choose between more national use of authority and personal privacy"
Alan Westin 1971[1]

1. Surveillanced/disciplinary society. Privacy and Digital Technologies

After Foucault and Agamben's analysis of biopower and biopolitics it can be said: Leviathan exists and it is greatly fine, we live in a disciplinary and normalized society, a society of ongoing surveillance where human rights are defined arbitrarily and everyone can be regarded as a Stanger about whom not only the state or its officials but also others want to know as much as possible. Life in modern society is life in the new "splendid" – a new Panopticon. Everyone can see everyone, but simultaneously a few (non-visible to others) might see the others.

Michel Foucault devoted his works entitled *Discipline and Punish: The Birth of the Prison* (1975) and *Society Must Be Defended* (1976) to the issue of disciplinary power. Discipline creates four types of individuality through: cellular (spatial distributions), organic (codes activities), genetic (accumulates time), combinatory (composition of forces). Disciplinary power elaborated techniques of special parcelization of the bodies based on the division, order, arrangement, placement and, as a result, the increase of control. These techniques were: 1) drawing up tables – hierarchical observation; 2) imposing exercises – normalization; 3) prescribing movements – normalizing

[1] A. Westin, Civil Liberties Issues in Public Databanks, (in:) Information Technology in a Democracy, ed. by A. Westin, p. 310.

ISBN 978–83–7431–363–6 ISSN 0860-150X

judgement; 4) forging new collective identities – disciplinary institution.[2] Those bodies were to be visible at the same time.

In what situation, as individuals and society nowadays, do we find ourselves? What is the contemporary Panopticon? What are the technological measures of vision/hearing/recording/ observation/monitoring/controlling/supervising an individual? The answers to these questions are at least partly universally known.

Placed in the iPhone and iPad, running with i0S4 system, a file called "consolidated.db" gathers user's geolocation data, in other words "tracks" his/her movement along with the date and time. If the programme "iPhone Tracker" is installed on one's iPhone or iPad (free access), one can depict on a map data which has been saved on that file – a court order is not needed anymore. Previous models of the iPhone also collected such data in an h-cells.plist file. Accepting the regulations, the user agreed to such a "track". The question is: how many users had read the regulations and knew about such a possibility? It should be assumed only a few of them. Most smartphones have a built-in GPS chip, which allows tracking a device and its user. Due to the fact that GPS works slowly, Apple and Google combine with each other data from flagpoles and wireless networks that are available nearby. Such databases had already been formed in 2008 by a company called Skyhook Wireless – with neither legal basis nor control. Currently, such data is collected by Chrome (Google) and Safari 5 (Apple). Also, this allows localizing a computer or a laptop. Additionally, browsers use programmes aggregating a user's online activity, creating his/her identity profile knowing a user's online history. There are applications such as Foursquare, Gowalla, that inform our acquaintances about our whereabouts. After publication of this information in the media in 2011, Apple ensured that it was a software error and from then on, those files would be encrypted and not be kept on the iPhone for more than a week. Have they kept their word? For many years, YouTube has reserved the right to use, duplicate, distribute, and work out or display contents that are placed on their website.

Facebook aggregates the data placed on its user profiles, and allows other people to track their acquaintances' identity profiles. One can only suspect that Facebook sells the collected data to insurance and advertising

[2] M. Foucault, Discipline and Punish: the Birth of the Prison, trans. Alan Sherdan, Vintage/Random House, New York 1979, pp. 136–170. See also: A. Schwan, S. Shapiro, How to Read: Foucault's Discipline and Punish, PlutoPress, London 2011, pp. 97–139; S. Oliwniak, Biopolitics and the rule of law, (in:) Axiology of the Modern State Under the Rule of Law. Selected Issues, ed. by S. Oliwniak, H. Święczkowska, Studies in Logic, Grammar and Rhetoric 19 (32), University of Bialystok 2009, pp. 33–48.

companies, simultaneously refusing to give back the information that had been placed by a user even after deletion of a profile. At the beginning of 2012, without users' consent, Facebook amended the profiles' privacy settings to the commonly available – and from then on users must change their privacy settings by themselves. How many users actually do this?

Since March 1st, 2012, Google has changed its privacy policy. Data concerning users of their products has been gathering beforehand, but ... Currently, data from all Google services are used to create a user's profile, the browser should identify a user's preferences and suggest appropriate or personalized advertisements and information. There are serious doubts regarding data protection and the way it is being used. Such a situation has drawn the Polish Inspector General for the Protection of Personal Data and the French CNIL's attention, also the attention of their counterparts from Canada, Germany, Israel, Italy, Ireland, the Netherlands, New Zealand, Spain, the UK, and the EU Commissioner for Justice Viviane Reding. Google does not see a problem, and claims that "in the privacy policy we have managed to find a reasonable balance" – Peter Fleisher, general counsel for Goggle privacy. However, not all data that is integrated can be controlled.

One may cancel their account on Google websites (80% of browsers on the market in Europe); how many users will do this, valuing highly the right to privacy rather than one's own convenience? A phone user with an operating Google Android system (52.5% of phones on the market according to the data from January 1st, 2012) practically can not log out of it. Another example: Intelius application for iPhone, a "dirt detector" sleaze detector – one puts down the name and surname or phone number of a newly acquainted person or pastes their "digital photo" and gets access to his/her tweets, information on criminal records, people living at the same address, the surface of his/her residential property and its status, his/her activity on Facebook and websites that he/she looks through. Google Street View records fragments of data that are being transmitted from wireless networks from houses being passed at that particular moment.

Also we have biometric technologies. They include a number of measures of human physiography as well as DNA: descriptions used in passports, such as height, weight, colour of skin, hair, eyes, visible physical markings, gender, race, facial hair, wearing of glasses; natural physiography e.g. skull measurements, teeth and skeletal injuries, thumbprint, fingerprint sets, handprints, iris and retinal scans, earlobe capillary patterns, hand geometry; biodynamics e.g. the manner in which one's signature is written, statistically analyzed voice characteristics, keystroke dynamics – particularly

login-ID and password; social behaviour, supported by video-film e.g. habituated body signals, general voice characteristics, style of speech, visible handicaps and god-tags, collars, bracelets and anklets, bar-codes, embedded microchips and transponders. Raymond Wacks writes: *"the biometric may then be used either to identify the subject by matching his or her data against that of a number of other individuals' biometrics, or to validate the identity of a single subject".*[3]

Next: identity cards and identity smart cards with a chip containing the holder's particulars of birth, nationality, address, marital status, occupation, details of any spouse or children. These cards may have multi-application, such as e-certificate, library card functions, quality service. But as Simon Davies has written in 1996 *"a card will imperil the privacy of personal information".*[4] And also DNA databases, technology of radio frequency identification (RFID) has emerged as a means of inventory control to replace barcodes. Combining RFID and wireless fidelity networks or CCTV cameras could facilitate realtime tracking of objects or people inside a wireless network, such as hospital. There are likely to be calls for sex offenders, prisoners, illegal immigrants, and other "undesirables" to be tagged.[5] As Foucault defines in "Discipline and Punish": *"the mechanisms of the disciplinary establishments have a certain tendency to become 'de-institutionalized', to emerge from the closed fortresses in which they once functioned and to circulate in a 'free' state; the massive, compact disciplines are broken down into flexible methods of control, which may be transferred and adapted."*[6]

Jack Schmidt, Google, spoke: "Privacy does not exist", as did Scott McNealy, CEO of Sun Microsystems: "Privacy is dead. Get over it". Is this really true?

Abandon the hope of privacy, those who log in in here – should such a warning be placed on Facebook, Google, Twitter, Bliper, Our Class websites, etc.?

Deliberations on the nature of the right to privacy in today's world, in cyberspace, are an old issue in a new format. It's about setting the limits of politics, designation of areas of private/public behaviors. After analyzing Baudrillard's concepts we may state a question: does reality exist? Following Manuel Castells we wonder: do we still cope with virtual reality, or rather do

---

[3] R. Wacks, *PRIVACY. A Very Short Introduction*, Oxford University Press, New York 2010, p. 10.

[4] S. Davies, Big Brother, Pan Books, 1996, p. 139.

[5] R. Wacks, PRIVACY, op. cit., p. 28.

[6] M. Foucault, *Discipline and Punish*, op. cit., p. 181–182; 211.

more and more people live in virtual reality? The answer to these questions requires a re-interpretation of current understandings of privacy, intimacy, solitude. Also, it requires re-pondering the freedom and autonomy of a human being in a network society, in cyberspace. It requires re-defining the borderline of individual freedom in the context of other individuals' freedom and the necessity to fix, once again, the limits between the freedom and the privacy of an individual and the common weal/public safety. Can we still use the concepts of John Stuart Mill, who in his essay "On Liberty" wrote: *"the sole end for which mankind are warranted, individually or collectively in interfering with the liberty of action of any of their number, is self-protection. That the only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others. His own good, either physical or moral, is not a sufficient warrant"*.[7]

What is privacy?

The value of privacy as a general moral, social, psychological or political value is undeniable, but the more the notion is stretched, the greater its ambiguity. An acceptable definition of privacy remains elusive.

Privacy can be defined on the philosophical plane as such an element of the freedom and the autonomy of an individual, which we may call solitude, or the state in which one decides about themselves, without the participation and influence of others. Privacy is a human property.[8] Simultaneously, it can be understood as a mental state, as intimacy, necessary also in relationships with other people, including marriages. It is also capable of deciding who and what possesses information about ourselves and to what extent this information is accessible to the public. It is also a space of our personal creation, artistic creativity, a space also in the purely physical dimension, free of presence, manipulation, domination, and the supervision of other people and state authorities. All the elements of privacy are listed by Alan Westin, who claims that "privacy gives individuals a chance to lay their masks aside for rest. To be always *"on" would destroy the human organism"*.[9]

Is privacy today, in cyberspace, where everyone, to a lesser or greater extent has fallen into the trap of network systems (everyone is "networked"), still of great value? Do young people, cyber natives, for whom cyberspace is

[7] J. S. Mill, *On Liberty*, Longman, Roberts & Green, London 1869, p. 9.

[8] About the philosophical and anthropological aspects please see. M. Chrabonszczewski, Privacy. Theory and practice, Oficyna Wydawnicza ASPRA-JR, Warsaw 2012, pp. 19–80.

[9] A. F. Westin, *Privacy and Freedom*, Atheneum, New York 1967, p. 34–35.

no longer a virtual reality – not virtual reality, but simply the reality which they occupy – need privacy? After all, for many their appearance in the network is an essential condition of their existence. They sell their privacy and intimacy voluntarily, because it is the only way to become known. They do not analyze the risks, even do not understand them, unthinkingly providing information about themselves and their personal photographs.

Samantha Miller writes *"In the digital world of online social networks users have grown accustomed to the free flow of information and expansive opportunities for self-expression".*[10]

According to Helen Nissenbaum *"we have a right to privacy, but it is neither a right to control personal information nor a right to have access to this information restricted. Instead, it is a right to live in a world in which our expectations about the flow of personal information, are, for the most part, met."* She called this right *"contextual integrity, achieved through the harmonious balance of social rules, or norms, with both local and general values, ends, and purposes. The framework of contextual integrity rejects the private/public dichotomy as a sound basis for a right to privacy and along with it the attempt to define* a category of sensitive information deserving special consideration".[11]

Are we dealing simultaneously with new forms of exhibitionism and voyeurism as usual attitudes online? It might not be important to them, in a state of apathy about their privacy, as the society is used to the omnipresence of CCTV (closed-circuit television) cameras and have accepted the rules of being kept under surveillance and being overseen.

Wolfgang Sofsky writes: *"People have long since gotten used to video cameras, discount cards, and advertising messages... Although it occasionally annoys him, the transparent citizen appreciates how much easier life is in the computer age. He unhesitatingly forgoes being unobserved, anonymous, unavailable. He has no sense of having less personal freedom. He does not even see that there is something to defend. He attaches too little importance to his private sphere to want to protect it at the expense of other advantages. Privacy is not a political program that can win votes... People leave more traces behind than they realize. No longer is one allowed to withdraw from society and live without being pestered.... The individual cannot secretly change masks and become someone else. He can neither dis-*

[10] S. Miller, The Facebook Frontier: Responding to the Changing Face of Privacy on the Internet, Kentucky Law Review 2008–2009, vol. 97, p. 541.

[11] H. Nissenbaum, Privacy In Context. Technology, Policy and the Integrity of Social Life, Stanford Law Books 2010, pp. 231–232.

guise himself nor temporarily disappear. His body is regularly X-rayed, his journey through life recorded, and his life changes documented... Nothing is overlooked, ignored, thrown away... When every careless act, every error, every fleeting trifle is recorded, there can no longer be any spontaneous action. Everything one does is evaluated and judged. Nothing escapes surveillance. The past suffocates present. If data were not erased at regular intervals, people would be imprisoned in the dungeons of their own history. However, this outlook seems to frighten hardly anyone".[12]

A legal right to privacy

Amitai Etzioni, in his *The Limits of Privacy* discusses three stages of development on the right to privacy: 1) pre-1890: utilizing principles derived from property rights to protect privacy; 2) 1890 to 1965: the right to privacy became a part of tort law; 3) post-1965: a major expansion of the right to privacy, particularly with regard to its constitutional rights.[13] The marker in the legal history of privacy is an 1890 essay by Samuel D. Warren and Louis D. Brandeis "The Right to Privacy". They framed their argument in terms of "the right to be let alone". The right to be let alone stands supreme and apart from other considerations; it presumes that all people can be left alone as much as they desire – completely if they so prefer – without restricting other persons' abilities to exercise their own right to be left alone to the fullest contest.[14]

At the start of the 20th century the Fourth Amendment was useless as a protection against subtler and more far-reaching means of invading privacy. In Katz v. United States (1967) the Supreme Court established a new standard for characterizing the Fourth Amendment also establishing *"a reasonable expectation of privacy"* standard for determining whether a Fourth Amendment violation had occurred. This "reasonable expectation of privacy" arises from the property right "to exclude others". "If surveillance does not invade the individuals' right to exclude others, the surveillance generally does not violate his reasonable expectation of privacy".[15] Today Jack

[12] W. Sofsky, *Privacy: A Manifesto*, Princeton University Press 2008, pp. 7–8.

[13] A. Etzioni, *The Limits of Privacy*, Basic Books, New York 1999, p. 189.

[14] S. D. Warren, L. D. Brandeis, "The Right to Privacy", *Harvard Law Review* 1890, vol. 4, pp. 289–320. See also: J. Sieńczyło-Chlabicz, Legal Discourse Surronding the Institution of the Right to Privacy – a comparative approach, (in:), Language, Law, Discours, ed. by M. Alksandrowicz, H. Święczkowska, Studie in Logic, Grammar and Rhetoric 26 (39), University of Bialystok 2011, pp. 197–214;

[15] O. Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, *Michigan Law Review 2003–2004*, vol. 102, p. 812.

Balkin claims that, *"the government aims to obtain any and as much information to possible, and, as a result, Fourth Amendment protections often are inadequate. ... Electronic surveillance is not its only tool. ..Government can also get information out of human bodies. Bodies are not simply objects of governance, they are rich sources of information that governments can mine through a multitude of different technologies and techniques"*.[16] One of the most significant components of the surveillance today is data mining. The government has the ability to obtain and analyze recorded information about citizens. Jeffrey Rosen describes *"Before September 11th, the idea that Americans would voluntarily agree to live their lives under the gaze of a network of biometric surveillance cameras, peering at them in government buildings, shopping malls, subways and stadiums, would have seemed unthinkable, a dystopian fantasy of a society that had surrendered privacy and anonymity"*.[17] Technology allows governments to deploy modern panopticism as a form of "subtle coercion" and the Fourth Amendment may be no longer an adequate safeguard.[18]

Daniel J. Solove indicates two models for the Protection of Privacy:

1) The Invasion Conception: from S. Warren and L. Brandeis. The primary remedy for privacy invasions should be a tort action for damages, and to a limited extent, injunctions and criminal penalties. Under this concept, privacy is understood as a series of discrete wrongs-invasions – to specific individuals. Solove notes that *"the invasion conception's focus on privacy invasions as harms to specific individuals often overlooks the fact that certain privacy problems are structural – they affect not only particular individual but society as a whole. Privacy cannot merely be enforced at the initiative of particular individuals. Privacy should be viewed as a constitutive value"*.[19]

2) Architecture – the protection of privacy depends upon an architecture that structures power, a regulatory framework that governs how information is disseminated, collected and networked.[20]

---

[16] J. Balkin, The Constitution in the National Surveillance State, *Minnesota Law Review 2008–2009*, vol. 93, p. 1–6.

[17] J. Rosen, A Watchful State, *New York Times Magazine*, October 7th, 2001.

[18] A. Sarat, L. Douglas, M. M. Umphrey, Itroduction: Change and Continuity – Privacy and Its Prospects in the 21st Century, (in:) *Imagining New legalities. Privacy and Its possibilities in the 21st Century*, ed. by Austin Sarat, Lawrence Douglas, Martha Merrill Umphrey, Stanford Law Books 2012, p. 8.

[19] D. J. Solove, *The Digital Person. Technology and Privacy in the Information Age*, New York University Press 2004, p. 97.

[20] Ibid, pp. 97–101.

Recently, in human rights' philosophy, growing acknowledgement is given for the thesis that it is not dignity, but freedom which is the objective basis of all rights and freedoms.[21] Freedom is expressed primarily in having the possibility of self-determination. In an ontological meaning self-determination of ourselves equals bearing the hallmark of being a person.[22] Self-determination constitutes the opportunity to decide about one's future, to wield one's existence and its dimensions: life and relationships with other people (the right to solitude, freedom to choose a way of one's life).

The legal definition of rights to self-realization of a human being, one's autonomy and privacy, is a consequence of a particular political philosophy, taken as an axiological basis of definite political order. The definition of freedom and privacy differs depending on if it is adopted by liberals or by communitarists. This is due to the fact that they define differently the right (principles of freedom or entitlement).[23] Also, privacy is not one of the notions which the semantic denotation is easy to define.[24]

The analysis of the concepts formulated in US doctrine results in the recognition of privacy as: 1) one's right to be let alone; 2) the limited access of others to an individual, eg. protection from the unwanted interference by the third parties; 3) control over private information; 4) respect for a private secret; 5) respect for intimacy.[25]

But in the digital age new communities are established and new identities formed, and the threat of intrusion into the private domain no longer originates primarily or exclusively with the state.[26] Robin Feldman argues

---

[21] For example W. Sadurski, A status of an individual in the eyes of the law: legal and philosophical thoughts on the legitimacy of procedural democracy and T. Kozłowski's opinion expressed in discussion, (in:) M. Wyrzykowski, Rights become law. A status of an individual and a developmental tendency for law, Liber, Warsaw 2006, p. 20–24.

[22] J. Hervada, A. Dorabialska, The natural law. Introduction, a crowd, PETRUS Publishing, Cracow 2011, p. 53–56.

[23] See broader: M. Paździora, Spór o prawa człowieka – jednostka, wspólnota, społeczeństwo, (w:) A. Sulikowski, (red.), Z zagadnień teorii i filozofii prawa. W poszukiwaniu podstaw prawa, Wrocław 2006, s. 85–100.

[24] See for example J. Braciak, Prawo do prywatności, Wydawnictwo Sejmowe, Warszawa 2004, pp. 21–28.

[25] D. J. Solove, Conceptualizing privacy, California Law Review 2002, vol. 90, p. 1094.; idem, Understanding Privacy, Harvard University Press 2009, pp. 14–38. In Polish literature: K. Motyka, Prawo do prywatności i dylematy współczesnej ochrony praw człowieka, Oficyna Wydawnicza Verba, Lublin 2006, pp. 19–136 writes broadly about the evolution of the understanding the right to privacy in the doctrine and jurisprudence of the U.S. Supreme Court.

[26] J. Cohen, Privacy, Visibility, Transparency, and Exposure, University of Chicago Law Review 2008, vol. 75, p. 181.

"It is *the fluidity of our interactions in modern society that makes us particularly vulnerable and requires special attention to the protection of the individual. The battered doctrine of public and private spheres is inadequate for such purposes, and our attempts to apply that doctrine in modern context is producing strange and unsatisfying results"*.[27] And adds *"modern communication and information issues do not map well onto traditional notions of the public and private spheres. Our instinct to address those issues by stuffing them into public/private boxes is already leading to strange, almost schizophrenic results. Consider our approaches to cyberspace. In some circumstances, we treat cyberspace as if it was analogous to a public domain, and in other circumstances, we treat it as if it was analogous to a private domain"*.[28]

Feldman argues that technological advancements have blurred the boundaries between the individual and society and confused the relationship between sovereign and citizen. The conceptualization of public and private spheres may no longer be adequate to address those challenge. It demands reconceptualizing the issues of control embedded in any discussion of privacy in the information age. We should view Internet interactions as consensual agreements, in which individuals will negotiate for those protections they desire, which reflects an outdated mode of thinking in which dangers are conceptualized as coming from single points, and the goal is to mitigate the danger by controlling those points.[29]

Julie E. Cohen presents civil libertarian arguments about privacy. Many such arguments privilege freedom of choice, including choices to surrender personal information in ways that may commodify the self. The notice-and-consent model, which facially appears to privilege liberty, concentrates all of the costs of controlling disclosures of personal information on the affected individuals. Some have criticized the liberty/efficiency binary that dominates debates about responsibility and accountability precisely because it avoids the problem of ethical responsibility toward others. Cohen writes: *"the current evolution of networked digital technologies is reconfiguring technology users to be passive consumers of media content and eager participants in the semantic web and the surveillance processes that feed it"*.[30] And she

[27] R. Feldman, Coming to the Community, (in:) Imagining New Legalities, op. cit., p. 86.

[28] Ibid, at p. 95.

[29] Ibid, p. 99.

[30] J. E. Cohen, Configuring the Networked society, (in:) Imagining New Legalities, op. cit., p. 139..

adds that *"government plays an important role in validating private technology processes, and not only because legal rules determine the 'public' and 'private' labels. Government actors are customers for technology products and services, and also are interested in advancing policy agendas of their own"*.[31] Jody Freeman proposes embracing the public role in privatized governance by reconceptualizing governance through the lens of contract, as an extended process of public/private negotiation because the traditional tools of government are neither the only nor the most useful tools for pursuing the implementation of public values.[32]

With regard to the legal regulation of cyberspace and protection of the right to privacy, it should be distinguished:

1) cyber-paternalism (statism) – it is only the state as a political organization which is authorized to issue the law and regulations regarding users' online activity, because the activity has its effects on the state territory.
2) cyber-libertarianism (separatism) – given the nature of the network, its users should form their own normative orders that are independent of the state.[33]
3) indirect stand – regulations of the network should combine both the users' and the state activity. Relations among network participants are the relations among anonymous entities, often short and unstable. These are not the multilateral legal relations based on civil law doctrine, but the network structures which are not normalized by any of the juridical theory.[34]

A different approach to network regulations is a consequence of the differences between American and European legal culture. Also, the understanding of the public and private spheres differs. In European legal consciousness formal arguments play an important role along with the search for the source of law, which have been previously established by the public authorities.[35] In the US the public/private distinction has to be under-

[31] Ibid, p. 141.

[32] J. Freeman, The Private Role in Public Governance, *New York University Law Review 2000*, vol. 74 (3), pp. 543–675.

[33] A. Murray, *Information Technology Law: the law and society*, Oxford University Press, New York, 2010, p. 56.

[34] K. Dobrzeniecki, Lex informatica, Wydawnictwo Adam Marszałek Toruń 2008, pp. 124–125; ibid, Prawo i etos cyberprzestrzeni, Wydawnictwo Adam Marszałek, Toruń 2004.

[35] See: A. Sebok, L. Trägård, Adversial Legalism and the Emergence of a New European Legality: A Comparative Perspective, (in:) *Imagining New Legalities*, op. cit., pp. 154–187.

stood as a series of commitments and contestations along multiple dimensions: state/society, individual/group, right/power, property/sovereignty, contract/tort, law/policy, legislature/judiciary, objective/subjective, reason/fiat, freedom/coercion.[36]

Since the beginning of the 1990s there has been a discussion if cyberlaw is an autonomous or separate normative order in relation with national law among the branches of domestic law. The prevailing position emphasizes the specificity of the network and the lack of adequate rules clarifying methods of its regulation. Justine Hofmokl remarks that so-called institutions managing a common pool of goods are a mixture of quasi-private or quasi-private institutions that are beyond the classical dichotomy.[37] It should be underlined that "the development of technology consistently overtakes the authors' idea of draft regulations. In such conditions interpretation of the law seems to be a difficult task.[38]"

According to the preamble to the European Community's Privacy Directive of 1995 "Whereas the difference in levels of protection or the right and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member State may prevent the transmission of such data ... whereas this difference may therefore constitute an obstacle to the pursuit of a member of economic activities ... distort competition and impede authorities in the discharge of their responsibilities".[39]

The European Union has put a lot of effort into the legal protection of Internet users since 1996. In January 1999, the European Parliament and the European Council adopted a resolution on illegal and harmful content on the Internet. Based on the above-mentioned fact, the program: Safer Internet Action Plus (1999–2004) and its subsequent editions from 2005 to 2008 and from 2009 to 2013 have been worked out.[40]

---

[36] D. Kennedy, The Stages of the Decline of the Public/Private Distinction, *University of Pennsylvania Law Review, 1982*, vol. 130.

[37] J. Hofmokl, Internet jako dobro wspólne, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2009, p. 77–87. See also: J. Kulesza, Ius internet. Między prawem a etyką, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2010, pp. 218–264.

[38] K. Dobrzeniecki, Lex informatica, op. cit, p. 52. See also: J. Janowski, Cyberkultura prawa. Współczesne problemy filozofii prawa i informatyki prawa, Difin, Warszawa 2012, pp. 304–328.

[39] Directive 95/46/EC of the European Parliament and the Council of October 24th, 1995.

[40] In greater detail these issues are discussed by M. Grabowska, The protection of Internet users in the European Union member states, KUL Publishing, Lublin 2012, pp. 193–266.

In the judgment of July 27th, 2004, the case Sidabras and Dziautas v. Lietuva the European Court of Human Rights adopted a broader understanding of the right to privacy than the Anglo-Saxon notion of "privacy". The right to a life in privacy means a life free from unwanted external interest. In its judgment of April 10th, 2007, the case of Evans v. United Kingdom the Court adjudicated that the state has an obligation to take action in order to create a framework for ensuring an individual the respect of their autonomy not only by public authorities but also by other private entities.

There is a need not only to regulate cyberspace, but also the digital data processing, artificial intelligence, intelligent agents, the processing of data generated by CCTV cameras, drones, and the scope of surveillance by public authorities or by host providers and other network users.

A surveillance camera has the capability to zoom in and read the pages of a book you have opened while waiting for the train in the subway. It can tilt, pan, and rotate – making it increasingly easy to track you as you move through your day. Facial recognition software is able to capture your image from the faces in the crowd, and then compare the image or your face against the facial images stored in law enforcement database. But also video cameras help protect the Public from Police Abuse.[41] In Poland, the European CCTV Indect system is being tested. It can not only recognize passers-by faces, but also record their conversations and analyze their atypical behaviors. Wojciech Rafał Wiewiórowski, the Inspector General for the Protection of Personal Data, observes that there are no regulations in this field, and it is necessary to supervise monitoring, as in Spain, Belgium, the Czech Republic and Italy.[42] Similarly, in Poland there are no legal provisions governing the monitoring of municipalities. In Polish legal order, only trade regulations apply that allow the application of monitoring, including simultaneous video and audio recording. According to the Ministry of Internal Affairs and Administration, the legal basis is the Act on Local Government.

According to the Council of Ministers' Directive of December 16th, 2009 on observation and registration with the usage of video technical means by

---

[41] See: The New York Civil Liberties Union, The Right of Privacy Is Destroyed by Video Cameras in Public Places and K. Mangu – Ward, Video Cameras Help Protect the Public from Police Abuse (in:) *Are Privacy Rights Being Violated*, ed. by R. D. Lankford, Greenhaven Press 2010, pp. 10–22.

[42] S. Jedynak, Video cameras track people without any control, "Rzeczpospolita" of September 27th, 2011, p. C3.

municipal police,[43] the municipal police are entitled to observe and record events that take place in public areas with the usage of technical means. However, this must be in regard with the protection of municipal facilities and the protection of public order. Also according to the Act of April 6th, 1990 concerning Police, art. 15 paragraph 1 point 5a,[44] it is entitled to use monitoring in public areas. Wojciech R. Wiewiórowski, Polish Inspector General for the Protection of Personal Data, again emphasizes that "According to the Article 29 Working Group the usage of video surveillance should respect the principle of proportionality. It means that, when other preventive and protection measures not requiring video recording are insufficient or impossible to implement, all tools used for such supervision should only be used as auxiliary measures. The authorities that are responsible for the collection and preservation of camera records must comply with the law on the protection of personal data, which might be difficult. It is not always clear how to apply properly the rules governing security vested with special administrative powers or people who are actually involved. Therefore, monitoring requires regulation."[45].

In 2000, the UK enacted the Regulation of Investigatory Powers Act (RIPA). Pursuant to the Act public authorities may ask Internet service providers for access to certain data that has been collected, if such information is acknowledged necessary for the protection of national security. The competence of public authorities is broad and indefinable.

The nature of threats to privacy posed online is defined as Privacy 2.0.[46] For example, using face recognition software, the program Picasso allows checking one's identity on a photo submitted. Similarly, web portals such as Polar Rose and MyHeritage combine images with data gathered on Facebook, Our Class and other websites. Protection of personal data such as cookies, e-mail addresses, IP addresses.

There is a widespread belief about the necessity to develop effective mechanisms for the protection of privacy online. Since domestic cyberlaw created by the state is difficult because of the above-mentioned specificity of the network (autonomy and users' multiplicity, the possibility of fast multiplication and duplication of information gathered on servers that are beyond state jurisdiction – the Internet deterritorialization), the legal basis might

---

43 Journal of Laws from 2009, No. 220, item 1720.

44 Journal od Laws from 1990, No. 30, item 179 with the following changes.

45 "Rzeczpospolita" of August 17th, 2011, p. C 6.

46 J. Zitrain, The Future of the Internet – And How to Stop It, Yale University Press 2008, p. 200.

be the rules and regulations adopted by the users themselves (netiquette, Creative Commons, Platform for Privacy Preferences – P3P Project). The possibility of digital reputation bankruptcy[47] or in other words the "right to forget" has been raised.

The European Commission is drawing up a bill that will replace Directive 95/46/EC. It will enter into force in 2014 or 2015. Pursuant to new provisions the administrator will be obliged to remove a user's data completely, such as name and surname, Social Security number, and address, and to check if data has not been transferred to other sources. If this has happened, the administrator will have to take action in order to remove it completely. Data processing will be possible only for a limited period of time (3 or 5 years). After this period, if the consent to data processing will not be extended, it will be deleted. Indefinite processing will be prohibited. The Inspector General for the Protection of Personal Data will be entitled to impose a penalty of up to one million Euros or 5% of the annual turnover on an entity which fails to comply with the new regulations.

We mustn't forget that every Internet user, regardless of the development of the legal framework for the protection of privacy online, should themselves control the information that they place online. Care of the self (in the sense laid out by Foucault) is inherently a mode of letting oneself be observed by others, and this observation can be coupled to systems of control. As Boris Traue writes: *"the qualitative difference between 'caring control' and 'cybernetic control' is that care (in the sense of cura sui) is retroactive... cybernetic control is pro-active"*.[48]

James B. Rule in his 1973 book titled Private Lives and Public Surveillance proposed the idea of a "total surveillance society". In 2007 he wrote *"the world clearly traveled well along the road toward total surveillance. The proportion of populations covered by systems of mass surveillance; the number and variety of points in life where such systems take in data; the subtlety of the judgments they afford and the effectiveness of the action taken on the bases of these judgments – all these things continue of rise"*.[49] And adds *"Without an unsentimental vision of the pressures on privacy, and the political will to confront them, the most ingenious legislation and policy-making*

---

[47] J. Kulesza, Ius internet, op. cit., pp. 111–112.

[48] B. Traue, The Cybernetic Self and its Discontents: Care and Self-Care in the Information Society, (in:) *Care or Control of the Self.* Norbert Elias, Michel Foucault and the Subject in the 21st Century, ed. by A. D. Bührmann, St. Ernst, Cambridge Scholars Publishing 2010, p. 173.

[49] J. B. Rule, *Privacy and Peril. How we are sacrificing a fundamental right in exchange for security and convenience*, Oxford University Press 2007, p. 163.

will avail little. It is not easy to opt for a messier, less efficient, more dangerous and unpredictable world as the price of authentic privacy. But the alternative is infinitely worse".[50]

Sławomir Oliwniak, Ph. D., Department of the State and Law Theory, University of Bialystok

[50] Ibid, p. 201.