SABINA BARANIEWICZ-KOTASIŃSKA*
Opole University
ORCID: 0000-0002-3545-6206

SLAWOMIR CZAPNIK**
Opole University
ORCID: 0000-0001-6479-5066

Surveillance in the liquid modern times

CYTOWANIE

Baraniewicz-Kotasińska Sabina, Czapnik Slawomir (2019). *Surveillance in the liquid modern times*. „Studia Krytyczne" nr 7: 11–23.

ABSTRACT

Surveillance, nowadays especially provided by information and communication technology, is at the core of social control that has been largely commoditised and privatized. Consumer culture gives hope for freedom lives, challenging the social hierarchies that dominated the earlier – in Bauman's vocabulary, "solid" – phase of modernity. The aim of this paper is to present two of many tools, which are used by biggest IT companies to keep under surveillance the individuals, societies and nations in the Liquid Modern Times. There has been the socio-cultural context of Internet's development analyzed to find the premises that led to a transformation of cyberspace from a freedom to a surveillance place, and conducted a case study of Facebook's facial recognition technology and Google Street View practices. Non-reactive research methods have been used in the paper.

KEY WORDS

surveillance, facial recognition, Facebook, Google Street View, liquid modern times

Introduction

To paraphrase famous, or rather infamous slogan of the Margaret Thatcher, there is no such thing as capitalism without surveillance,

* Instytut Politologii, Uniwersytet Opolski, ul. Katowicka 89, 45-061 Opole, Poland; e-mail: s.baraniewicz@onet.pl

** Instytut Politologii, Uniwersytet Opolski, ul. Katowicka 89, 45-061 Opole, Poland; e-mail: czapnik.slawomir@gmail.com

there are only invigilators and their tools. To be sure, it is not goal itself, but highly useful tool to extract wealth from its producers, working people. Every naive dream, that with new tools of digital production the class divide between producers and capitalist is overwhelmed, became useful fantasy, which conceals not-so-hidden truth: so-called prosumers (producers and consumers in one) in their comfortable chairs in front of a computer screen as as exploited as Adam Smith's labour in pin factory. There epitomize centuries-long capitalist desire to obtain effects of other people's labour without a money compensation paid to employee called wage.

Lack of understanding of this material reality is partly element of a broader situation of "liquid modernization", a concept developed by late Zygmunt Bauman (2000). We would like to remind, that this thinker developed concept of so-called "liquid surveillance" (Bauman 2012; Czapnik 2016). Long story short, in liquid phase of capitalism our situation is very unstable, volatile, insecure, and neoliberal ideology quite effective convinced many people, that collective action is absurd, and every is alone in a lifelong struggle – one may add, that "Alone again" is a title of one among Bauman's book (Bauman 1994). Surveillance, nowadays especially provided by information and communication technology, is at the core of social control.

In modern capitalist states, as Tony Blackshaw observes, social control has been largely commoditised and privatized. Consumer culture gives hope for freedom lives, challenging the social hierarchies that dominated the earlier – in Bauman's vocabulary, "solid" – phase of modernity. Liquid modernity operates within the system of power and hierarchy, which on the surface seems to contradict the sociological stratification of social class, gender and race. The freedom that embodies liquid modernity, is in the last instance the freedom to consume – the freedom to live and act without the participation of the society, transgressing the boundaries of class, gender, culture and ethnicity that could be a barrier to personal fulfillment (Blackshaw 2005: 119 –120).

The aim of this paper is not to show that there is no privacy in cyberspace, because we would only trivialize, as the problem is well known in our society. We just want to present the simple tools, which are used by biggest IT companies to keep under surveillance the individuals, societies and nations, what has been done on by the case study of Facebook's facial recognition app and Google Street View platform. To begin with the issue, there has been the socio-cultural context of Internet's development analyzed to find the premises that led to a transformation of cyberspace from a freedom to a surveillance place. Non-reactive research methods have been used in the paper.

The notion of surveillance

David Lyon, a Director of the Surveillance Studies Centre at Queens University in Kingston, Ontario, says that surveillance is just part of the way we run the world in the 21st century. The researcher defines that phenomenon as "purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection". In his definition Lyon points out four elements that describe the surveillance: 1) it is a purposeful attention, that means there is a justified point for watching, 2) it is a part of regular (it happens on our daily living) and 3) systematic procedure (it follows a planned schedule), and finally, 4) it focuses on personal details. As Lyon (2008) explains, such collected data may be then stored, transmitted, retrieved, compared, mined and traded.

Surveillance could be perceived a political technology of population management (Ceyhan 2012: 40), some kind of Focauldian *biopower*, important from a point of view capitalist society and formation of nation-state. In other words, surveillance cannot be described as new phenomenon – it has existed and has been developed since centuries as people always watched over each other. Those are the surveillance instruments that change depending on technological evolution, and new watchers that entrance the group of as well interested in consumer's and citizen's personal data. Thomas Allmer (2012: 11) observes, "Although there are a lot of other features in contemporary society as information, neoliberalism, globalization, capital, etc., surveillance in general and Internet surveillance in particular are crucial phenomena".

According to Gary T. Marx (2012: xiii), "A great deal was going on in the mid-1980s with the arrival of ever more powerful and seemingly omniscient, omnipresent knowledge machines. Consider video cameras; drug testing; computer documentation, discoveries, predictions and networks; location and communication monitoring; DNA analysis; and the many other new forms the current volume so richly documents. Violent and non-violent forms of social control were uncoupled, with the latter increasing in importance. Over recent decades subtle, seemingly less coercive, forms of control have emerged within societies that have not become less democratic and in which the state makes less use of domestic violence".

Undeniably, the emergence of the Internet had a huge influence on upgrading earlier available surveillance tools and creating new possibilities of spying, of which secret services could not even imagine that one day they will come true. What is interesting the most, as first it was not planned and not even aware that the network will evolve into an ideal platform for human, organizational, and national surveillance. This process of change will be now briefly, but not at length due to its complexity, described. The authors will mostly focus on the role of the

net users to analyze their behavioral influence on the change of Internet perception as the place ideal for an invigilation, as well as will indicate specific network characteristics that enabled and deepened the mentioned process.

According to Jason Pridmore (2012: 321), "Though the collection and use of consumer data are hemmed in to different extents by privacy regulations and data protection laws, the means by which consumers are surveilled is ever more innovative and enticing. Corporations are able to use the tools, processes and possibilities of new information and communication technologies, and employ rewards, discounts, entertainment, collaboration, special access, networking, recognition, better service and products, and coercion, amongst others, as mechanisms to produce detailed consumer-specific data".

The socio-cultural context of Internet's development towards a surveillance platform

In 1958, a year after the Soviet Union launched the first artificial satellite in space, the United States Department of Defense, fearing the aggression from the side of the Union of Soviet Socialist Republics, established the Advanced Research Projects Agency (ARPA). Its main task was to develop innovative technological projects that would strengthen the defense of the United States of America in the face of foreshadowing third World War and would ensure its military superiority over the enemy. One of such task was to create for military purpose a network that would be resistant to destruction and could survive any atomic bombing (Castells 2001: 10). The plan presumed a creation of decentralized network that would operate even in case of one of its components damage – under war conditions it could be theoretically safer like that. Today, this decentralization does not serve the security of virtual space, but creates chaos and prevents its ordering, and that builds good conditions for surveillance spread in the network. Paradoxically, this „order" corresponds with the main online stakeholders' goals – it is easier to adapt a space without a clear structure to the rules occurring in a commercialized, globalized world or to current political needs. Therefore, they maintain this lack of hierarchy, officially acknowledging this status as a value emphasizing freedom prevailing on the Internet.

In fact, at the very beginning, the Internet was seen by its users as an oasis of never-ending freedom along with its political control weakening at the turn of the 1960s and 1970s. It guaranteed liberty of speech, anonymity, the self-improve possibilities and a knowledge share. Its specific architecture allowed to break the communication barriers of the real world and enabled free use of network resources without anyone's control. The Utopians associated the Internet with a coming of

freedom age and the possibility of unfettered creation and conditions for direct democracy (Grossman 1995). They saw in it a liberation tool that would give people access to information making them independent above all from the state and large corporations (Castells 2001: 60–61).

In the mid-1990s, however, the US network was privatized. Although it gained the entrepreneurs recognition, it was still a paradise for utopians who believed in the anarchist freedom of the Internet. Its open architecture allowed connections with the whole world, and desktop computers, with the size similar to those of today, tempted with its price the individual users. After 2001, with the emergence of a broadband network, there started to appear the first social networking sites, the main representatives of Web 2.0 sites, that allowed ordinary web users to easily create and share content or comment, rather than only have access to data as before in Web 1.0 (O'Reilly 2005).

On this wave, the first social media, blogs, platforms for video exchange and other services were created – their main basis was interaction with the user. The initial boom, and even a certain trend of anonymity, the use of nicknames and the ability to adopt any identity on the Internet, have stopped being not so much popular as not functional. Hiding an actual personality was associated with the anarchist origins of the web as a place of freedom, self-realization, the possibility of being who the net users want to, deciding about themselves and the scope of disclosure of their data. People who discover their real name and surname have become more trusted in the Web 2.0. Anonymity became inconvenient mainly for cyber companies, which back then experienced their real flourishing due to the growing activity of Internet users in the network and the increasing information share.

Once recognizing the value of data, corporations have learned to make commercial use of them. That allowed cyber firms to slowly implement their market rules to the Internet, which is nothing surprising – this is how business works. An anonymous user has thus become less attractive for online platform providers, especially for those for who knowing the identity of their "client" means the possibility of better matching services and content to their needs and expectations. For this reason, companies additionally promoted all activities related to the disclosure of real data. The need of giving one's name and surname in the social network araised also from its specificity; by using a pseudonym, it would be harder to find friends online. In this way, the social network continued the old tendencies of the net under the pretext of freedom – slowly limiting it, used it more for commercial purposes.

At that time, the network users, who were fascinated not only by the benefits of using Internet services, but above all by the opportunities to find and deepen their contacts, began to transfer their real-life activities to the network. With the increase of its popularity, the physical Internet network amalgamated stronger with the social networks

created by its users (Lombard, Nahon, Sidhom 2008: 59), who began, as Castells (2001) describes, to use the Internet primarily to organize their social life. The multitude of these new digital technologies was the reason not only for the increasing use of the Internet – cybernauts completely "immersed" in these networks.

As a result of the unusual predispositions of the Internet, including abilities to respond to almost all human needs, both private and professional, in the most attractive way for people: quickly, easily, for free and effortlessly, it has become not so much useful, but almost essential to live technology. Our society have entered, as Didier Lombard determines it, into the ‚always on' era, where the Internet is always active and accessible, in which the network world blends with the world of people (Lombard, Nahon, Sidhom 2008: 82). Broadband access to the network also contributed into it, as it further enhanced the development of digital content and services consumption among users.

The networks began to influence our everyday life and propagate new cultural forms (Orliński 2013: 41). In this way, new media began to shape a new lifestyle, in which network users reveal their identity on the Internet much more than in real life: they publicly display information about their interests and preferences, and they scrupulously document every action taken in their lives. The society encouraged by the cyber firms is more willing to share all their private data. People exchanges opinions, searches for interesting information on the Internet, reveals their political views, family relationships, their relationship status and whereabouts. They wear health and activity monitoring devices, and publish their measurement results on various portals online. They also allow to track their location without even wondering what the purpose of this action is. Not thinking about the consequences, they leave with every click a lasting trace of their activity on the Internet. The liberty of shared content is so huge that it is impossible to control them anymore on our own. There has became the time of pictures, exhibitionism and selfie, which places an individual and its "attractive" life in the center of attention.

The life of the network society has become more transparent, but that creates an opportunity for its easy monitoring and – as a consequence – controlling. Paradoxically, each network users agrees on this terms every time they mindlessly accept with a click cyber corporation's privacy policy and regulations. Attracted by the ideas of freedom, people lost their vigilance, and corporations, seeking to commercialize the network more and more, make an use of it and freely invigilate individuals, societies and nations (Ippolita, Mancinelli 2013: 162). Nowadays, we live not as much in an information society or network society as much as in a surveillance society. The term of "surveillance society" was first used by Gary T. Marx in the mid-1980s, who wanted to describe the then situation, where the new technologies helped to crum-

ble the final barrier to total social control (Marx 1985). In this context, Lyon shows a paradox of a surveillance society: the people living in it, are not only constantly being watched, but they as well want to use technical devices to watch others (Lyon 2009). Since the liquidation of the barrier along with the Internet development, the surveillance techniques evolved rapidly. This concerns gathering information from our credit cards, mobile phones and computers, which accompany us in our daily life, but also tracking our moves through CCTV cameras, and other electronic devices, what obviously breaks human privacy rights. The watchers here are they all – the governments, organizations, corporations, and those about which we will never know.

In the next part of article the authors present two case studies of technologies that interfere into our privacy rights and are widely used for surveillance reasons – but of course in a public rhetoric it is not their main application. Both tools are very useful in our daily life. First – Google Street View, owned by Google Inc. (which is a part of the Alphabet conglomerate), is broadly used to find an exact address on a map, and check from the street point of view how the surrounding looks like. The second – face recognition, may be applicative when we want to quickly tag and find a friend in our virtual album or put a virtual, funny mask on our face by taking and sending a picture to our friends on Snapchat. As people do not think much about an interference of these simple tools with their privacy rights, the authors gathered and analyzed some examples of their abuse to show a civil threat that they may pose, and thus, to emphasize the need to – alone, take a better care on our privacy safety, because institutionally there is no chance for it.

The surveillance by Google Cars and through Google Street View

Eric Schmidt, former Google CEO, said once that people who do not like Google Cars taking pictures of their homes "can just move" (Paczkowski 2010).

Google Street View is a feature on Google Maps that allows you to walk virtually through the streets of different cities and view them in 3D. In 2010 it came to light that the entire fleet of Google Street vehicles, from cars to snowmobiles, responsible for photographing streets, houses, city centers and their peripheries, unknowingly, for three years had been collecting fragments of private information that people from around the world sent via unencrypted WiFi. These were, according to the company's relation: emails, URLs and passwords. Google quickly apologized for its mistake and assured that it would delete the data and fix the error in the code as soon as possible (Lee 2014: 86). However, the French data protection authority imposed a fine on Google because,

according to their investigation, the cars also illegally intercepted the passwords and details of online banking operations and medical prescription (CNIL 2011). How could the corporation for three years not notice that the machines provide them with additional information? It is hard to believe in the incidentality of this event, knowing that somehow Google had to process, organize and use this data – after all Google Cars collected it on some purpose. The French commission of the CNIL (fr. *Commision Nationale de l'Informatique et Libertes*) in its report stated that Google did not deny using the identification data of people gathered without their knowledge from WiFi access points (CNIL 2011).

This incident indicates that Google may consciously or not collect data of interest, without major consequences, because, what is the penalty of 100 thousand euro for such a company (that was the fine imposed on it by the CNIL)? As a remedy, it will apologize to its users, announce that it will correct errors and delete data, but we are not sure whether Google does it because simply those information are no longer necessary for the company after the three-year analysis. The price of such action will again be the take away of people's privacy, and for what this time they did not agree. It is terrifying that if this incident did not see the daylight, nobody would know that Google could have access to such private information. And how many similar "mishaps" have never came to light?

Unconscious collection of information for the Google Street View application is not the only problem. Wandering and taking pictures through half the world, Google cars captured people in underwear in their gardens and naked behind the glass windows of their homes. Immortalized scenes on nudist beaches, women entering abortion clinics and men into brothels. They witnessed attacks on the street, car accidents, thefts, fights and other incidents (Only a few pictures are to see at: Molloy 2016). The last instances may do have an impact on evidence in a case, but still all the photographs were taken without notice and permission to immortalize people in situations that can be ambiguously read and bring various consequences. First of all, they interfere with human privacy. It is understandable that all these photos have been taken from the street view, that means every passerby could accidentally see what Google car was at the moment (which is the company's defense line), but the probability of its immortalization and spreading on one of the most used sides of the world is definitely smaller. The corporation blurs faces and car registrations, however, the machines are not reliable and sometimes the algorithms blur objects captured in photographs mistakenly. Moreover, even blurred, the people's silhouettes has still such a good quality that its recognition by someone who knows them is not a problem. Anyone, who finds themselves on Google maps, can notify that fact to the company which will delete the photo.

The problem is that our right to privacy will be violated long before our image removing.

After the intervention of the European Commission, Google declared that it will publicize the information about the area documentation's time – in this way it cleverly unloaded the responsibility on others for staying in the same place and at the same time there, where Google Cars. It remains nothing than to hope that the corporation does not analyze face pictures from Street View's original photos, which are being stored to guarantee the quality and reliability of maps, and correct mistakes in the process of blurring faces (Google 2018), and does not connect them with location data and our identity to know where and on what purpose do we go to, to get to know better our behavioral figure. But after Schmidt revealed "We know where you are. We know where you've been. We can more or less know what you're thinking about (Saint 2010)" that hope is very fragile.

Alphabet, the parental company of the Google, prefers not lesser, but much, much higher degree of corporate surveillance. Among Google's patents are 'apparatus within a street lamp for remote surveillance' (patent number in United States – US08752566) and 'apparatus within a street lamp for remote surveillance having directional antenna' (US09265462). First item is "A covert surveillance system for viewing images from a remote location is provided. The surveillance system provides a mirror, lens and camera arrangement within a small enclosure which allows full 360 degree pan, tilt, zoom, focus and iris control from a remote location" ("Apparatus within a street lamp for remote surveillance", 2018). Second "system receives control commands such as rotate left, zoom out and tilt down via a radio receiver, and controls the camera accordingly. Images viewed by the camera are transmitted to a remote receiver for display on a monitor, or for recording" ("Apparatus within a street lamp for remote surveillance having directional antenna", 2018). We are powerless against the power of corporations.

Facial recognition technology as a threat for privacy

The photographs visible in Google Maps seemed harmless until the machines learn how to link photos with a particular name – Google's Picasa users know how quickly and effectively a machine can recognize faces. Paradoxically, those are the net users who helped to achieve that by sharing and tagging photos on the web.

Facebook also invested in face recognition technology. In 2012 it bought Face.com – a prominent supplier in that field. The software created by the company, as they convinced, was characterized by high accuracy and operated throughout the whole network. Their algorithms were able to identify faces despite such difficulties as poor light or blurry images. Glasses, beards or disguises were not a problem for them

(Lee 2014: 44). Thanks to this technology, Facebook can find now a human face in a picture within a second, and as a result of billions of photos analisis, very precisely match it to the owner. This allows the service to get even more information about a user – where they are, with whom, in what circumstances, what emotions they share. It is hard to wonder why the face detection technology quickly became that popular and found more purposes in other fields.

The first application that could recognize the face in real time was designed for Google Glass. It allowed it users to capture a stop-frame of face images that they saw through their glass and immediately find their owners. The system scanned photos available on social media and on dating sites (Lee 2014: 45). In this way, movie fantasies about super agents having access to science-fiction devices, have been transferred to reality, thus completely destroying human anonymity. This type Russian application "Find Face" has gained immense popularity not only among the users of the well-known social portal Vkontakte, but also among the Russian police. Suffice is to put a picture of a face in it, and within a second it will compare it with a billion of other photographs available on the social networks. During the period of its two-month existence, over half a million people registered in it. Initially, its aim was to help find a person who caught someone's eye in order to be able to make an appointment with them, but its application quickly checked well in the investigation department. The application developers have also started a cooperation with the Moscow authorities, which is to lead to the development of pictures analysis from the city monitoring network. It counts 150,000 cameras (Walker 2016).

As nowadays cameras are everywhere, face recognition technology should be considered as very controversial – cameras are in smartphones, in cities, in works, parks, and even homes. Inclusion of this technology in the monitoring system allows a constant tracking of naturally showing faces people. If this tool will be used only in cases justified by the course of an investigation and will seek to detect or prevent the offender, it might be useful. However, in the case when its abuse interferes with human privacy, such technology should have stronger restriction of an usage.

About such an excellent possibility of tracking the actions of individuals probably did not even dream of the service of the Security Service in the times of the Polish People's Republic – even then people, who were in danger of the authorities, could hide, change their identity, leave. Today, in the face of new technologies that supervise consumers, it would be extremely difficult, if not impossible to hide or simply escape from our previous, full of unpleasant experiences life. Face covering will also not help, because the experimental algorithm of Facebook is already taking a step forward – it will recognize a person even if they face is not in the picture. In order to determine the identity of a photo-

graphed person, it will help the company again something as innocent as a photo we shared with a sentimental meaning. For corporations it is a repository of knowledge. Based on its analysis, the algorithm can see our characteristic physical features such as hairstyle, clothing and body structure. That is enough for it to be able to identify anyone – during tests the application gained 83% of effectiveness (Anderson 2015).

Dissemination of this type of programs for general use will lead to the situation where everyone will be able to take a picture either in a restaurant, on vacation or on the street and get a direct connection to anyone's social profile, and this means often an access to such information like our places of residence, list of friends, interests, and to all other information that a search engine has indexed about us. Drawing conclusions about our person and an affluence will not be a big challenge on this basis. It will be a big lure for all kinds of criminals and facilitation for security services. The worst is probably the idea what pictures such an application could pick out from the depths of the network. After all, we did not put a lot of photographs on our own, some were shared by our friends in the "cloud" and some on social networks without even informing us about it. Moreover, on a large part of the photos we probably found ourselves quite by accident and we do not even know the photographer. We need to include into this numerating the photos from the youngest years, which were published on schools websites, as well as photographs of the institutions in which we worked and (the trend of recent years) from virtually all events we were involved in – organizers especially like to promote their activities on the web and they are happy to upload photos of people taking part in their event, even if it was fun at night club.

Lack of privacy, anonymity, and perhaps even embarrassment because of photos of very private situations, and possible repressions by the authorities – these are just some of the negative consequences of developing face recognition technologies that prepare for the netusers cyber corporations. That saw the users of the Polish social networking portal Nasza Klasa, who had long ago forgotten about their accounts and passwords after Facebook appeared on the horizon (or will just find out because the matter is fresh and not yet broadly publicized). The owner repaid them by publishing all forums and class galleries that previously users had added privately. They only need to enter their name in Google Search and it will return them terrifying results.

Conclusion

No doubts, we have to well aware about many approaches to privacy. Libertarians and liberala were highly effective in silencing other schools of thinking in the area of public understanding meaning of privacy. Their approach is important, but rather unuseful in current

liquid capitalism, it usually more neglected than revealed. According to Christian Fuchs, "The liberal conception of privacy (and its reality) as an individual right within capitalism protects the rich and their accumulation of more wealth from public knowledge. A socialist conception of privacy as a collective right of workers and consumers can protect humans from the misuse of their data by companies" (Fuchs 2012, p. 141). One may guess, that Bauman, lifelong socialist, would rather prefer socialist conception of privacy, which serves not capital, but human beings.

To put it simply, surveillance – as poor in Bible's parable – will always be with us. Honestly, it is not necessarily bad thing. Every care is more or less founded on gathering information by the caregiver about her or his ward – i.e. children playing in another room. But it is hardly surprise, that surveillance capitalism is phenomenon grounded in profit-seeking and nothing else. Every data its collect is potentially source of income, a way to commoditise human thought, actions and relationships. Every rational person, who is concerned with privacy and overwhelming and ever-expanding surveillance, have to think about its relations with global capitalism.

If you think, that we can curb not only excesses of surveillance, but try to break its own internal logic with its enormous negative impact on society, without curbing – or overthrowing – capitalist social system itself, think again.

Bibliography

Allmer T. (2012). *Towards critical theory of surveillance in informational capitalism*. Frankfurt am Main: Peter Lang.

Anderson M. (2015). *Facebook facial recognition algorithm uses more than your face to identify you*, https://thestack.com/security/2015/06/23/facebook-facial-recognition-algorithm-uses-more-than-your-face-to-identify-you [18.03.2018].

Apparatus within a street lamp for remote surveillance having directional antenna, https://patents.google.com/patent/US6624845B2/en [12.04.2018].

Apparatus within a street lamp for remote surveillance, https://patents.google.com/patent/US5886738A/en, [12.04.2018.]

Bauman Z. (1994). *Alone again: Ethics after certainty*. London: Demos Medical Group:

Bauman Z. (2000). *Liquid modernity*. London: Polity.

Bauman Z., Lyon D. (2012). *Liquid surveillance: A conversation*. London: Polity.

Blackshaw T. (2005). *Zygmunt Bauman*. Abingdon: Routledge.

Castells M. (2001). *The Internet Galaxy: Reflections on the Internet, business, and xociety*. Oxford University Press: New York.

Ceyhan A. (2012). *Surveillance as biopower*. [in:] Ball K., Haggerty K., Lyon D. (eds.). *Routledge handbook of surveillance studies*. Abingdon–New York: Routledge, 38–45.

CNIL (2011). *Délibération n°2011-035 du 17 mars 2011 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société X,* https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000023733987 [28.03.2018].

Czapnik S. (2016). *Liquid surveillanc*e. [in]: Blackshaw T. (Ed.), *The new Bauman reader: Thinking sociologically in liquid modern times*. Manchester: Manchester University Press, 364–387.

Fuchs Ch. (2012). The political economy of privacy on Facebook. *Television & New Media* 13(2): 139–159.

Google (2018). *Privacy Policy*. Google, https://policies.google.com/privacy [19.03.2018].

Grossman L.K. (1995). *The Electronic Republic reshaping democracy in the Information Age*. Penguin Group: New York.

Ippolita, Mancinelli T. (2013). *The Facebook aquarium: Freedom in a profile*. [in:] Lovink G., Rasch M. (eds.), *Unlike us reader, social media monopolies and their alternatives*. Amsterdam: Amsterdam Institute of Network Cultures, 159–165.

Lee N. (2014). *Facebook nation*. New York: Springer Science+Business Media.

Lombard D., Nahon G., Sidhom G. (2008). *The second life of network*. New York: Odile Jaco.

Lyon D. (2008). *Surveillance society David Lyon. Queen's University. Canada talk for Festival del Diritto, Piacenza, Italia: September 28 2008*, http://www.festivaldeldiritto.it/2008/pdf/interventi/david_lyon.pdf, 20.11.2018.

Lyon D. (2009). *Surveillance, power, and everyday life*. [in:] Kalantzis-Cope P., Gherab-Martín K. (eds). *Emerging digital spaces in contemporary society*. London: Palgrave Macmillan, 107–120.

Marx G.T. (1985). The Surveillance Society: the threat of 1984-style techniques. *The Futurist* June: 21–26.

Marx G.T. (2012). *Preface: "Your papers, please": personal and professional encounters with surveillance*. [in:] Ball K., Haggerty K., Lyon D. (eds.). *Routledge handbook of surveillance studies*. Abingdon–New York: Routledge, xx–xxi.

Molloy M. (2016). *13 bizarre Google Street View photos that will leave you confused*, http://www.telegraph.co.uk/news/2016/09/04/13-bizarre-google-street-view-photos-that-will-leave-you-confuse/ [28.03.2018].

O'Reilly T. (2005). *What is Web 2.0*, *http://*/oreilly.com/pub/a/web2/archive/what-is-web-20.html [02.03.2016].

Orliński W. (2013). *Internet. Czas się bać*. Warszawa: Agora SA.

Paczkowski J. (2010). *Schmidt: Don't like Google Street View photographing your house? Then Move*, http://www.allthingsd.com/20101025/schmidt-dont-like-google-street-view-photographing-your-house-then-move/ [17.03.2018].

Pridmore J. (2012). *Consumer surveillance: Context, perspectives and concerns in the personal information society*. [in:] Ball K., Haggerty K., Lyon D. (eds.). *Routledge handbook of surveillance studies*. Abingdon–New York: Routledge, 321–329.

Saint N. (2010). *Google CEO: "We know where you are. We know where you've been. We can more or less know what you're thinking about"*, http://businessinsider.com/eric-schmidt-we-know-where-you-are-we-know-where-youve-been-we-can-more-or-less-know-what-youre-thinking-about-2010-10?IR=T [17.03.2018].

Walker S. (2016). *Face recgognition app taking Russia by storm may bring end to public anonymity*, https://www.theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity-vkontakte [17.03.2018].