THE COLLISION BETWEEN PUBLIC POLICY AND TECHNOLOGY RAISES THE STAKES FOR USERS

Claudia GOGOAŞA LASCATEU*

Motto: *"Salus populi suprema lex esto"* [1]
(Iustinian I, 482 –565 a.D.)

Abstract

Strategy, public policy and threat management have risen and flourished despite the constant conundrum of protecting infrastructure and top technology. To have both the big picture and successfully prevent or interrupt malicious behaviour it is necessary to comprehend what the threat is and what it means to us, and to achieve that, we must be able to position ourselves between grasping what public policy has to offer and what technology brings to the table.

This is intended to be an interdisciplinary approach on law and policy that will show what are the limits and guarantees of user experience nowadays in the European Union and, secondly, will argue the advantages and disadvantages to what are users experiencing in non-member states.

The paper will analyse what part data and confidentiality for security plays and how a continuous development of policy and strategy can answer the questions raised by technology and hybrid threats to national security. It will follow the lines European policy draws given the latest threat development and will revolve around what changes form the user's perspective.

Therefore, from necessity to strategy, to enforcement, the first step is identifying and addressing one issue in a common manner. Furthermore, it means we can achieve common grounds and have a correct and adequate solution. In order to find out how public policy works better for individuals, we scrutinise whether the European General Data Protection Regulation (GDPR) is an answer to all our questions, or just a complex insurance designed to safeguard user online experience. Moreover, we study how enforcing an internet law like China or Russia is in comparison to having a set of rules and guarantees such as the European GDPR, and the effect on user digital behaviour.

* PhD candidate, "Mihai Viteazul" National Intelligence Academy.

[1] "Let the safety of the people be the highest law", Cicero, De Legibus, Loeb Classics, p. 467.

The basis of this study will approach European case law on the matter of guaranteeing user fundamental rights concerning confidentiality, showing how European strategy is being enforced by regulations and put into force by law. It also finds that member states have the inherent responsibility to guarantee both user rights and transparency.

To have a better understanding on how people perceive the rules and regulations we use polls to measure how the public policy framework is comprehended by the people it intends to protect, and if the state policy toolset guarantees users digital literacy.

Keywords: *user, privacy, personal data, law.*

Introduction

The right to have a protected intimate, family and private existence is complex and is guaranteed by the Romanian Constitution from the outset as a supreme value (Article 1 of *Romanian Constitution*, 2003), further enhanced by the complementary obligation of state authorities to respect and guard individuals and their privacy (Article 26 of Romanian Constitution, 2003). The state, through public authorities must employ whatever means necessary within reason to guarantee privacy of individuals as fundamental human right. These have roots in the International Covenant on Civil and Political Rights (ICCPR)[2] Article 17 which states that nobody can be subject to arbitrary or illegal pries in his private life, family or home, neither can be unlawfully offended in his honour or reputation. Every person has the right to be protected by the law against such transgressions.

Furthermore, the Romanian New Civil Code states that anybody has the right to live, to be healthy, to have mental and physical integrity, to have dignity, to have self-image, to have his private life respected, and these rights cannot be transmitted (Article 58 of the *New Romanian Civil Code*). These are fundamental human rights, guaranteed by the Romanian Constitution sprung from the International Bill of Human Rights. The Romanian law states that anybody is entitled to have a name and a place of residence legally obtained. So, these attributes are not guaranteed, as they are conditioned by the pursuit of legal procedure, but are qualities that are constituent of the fundamental right to live and have a private life.

[2] It is a multilateral treaty adopted by the United Nations General Assembly through GA. Resolution 2200A (XXI) on 16 December 1966, part of the International Bill of Human Rights, ratified by Romania in 1974 by Decree no. 212.

The limits and guarantees of user experience nowadays in the European Union

The protection of user privacy as a guarantee stated in Article 8 of the Human Rights Convention and Article 16 of the European Union Treaty is now better outlined and linked to responsibility and the requirement to implement a system of protective measures that cover both data bases with personal data and the limits and conditions of third-party exchanges.

For instance, the Romanian law has included a general interdiction (Article 65 paragraph 2 of the *New Romanian Civil Code*) for identification of a person based on his genetic fingerprint outside of a civil or penal suit or in a medical or research matter. It is concordant with the European Human Rights Courts` jurisprudence that basically outlines in the 2006 *Van der Velden v. the Netherlands decision* that Article 8 in the Human Rights Convention the right to respect one`s privacy covers the issue of retention of data related to biological features of an individual, beyond the scope of its submission in the first place, because it is protected under the 1981 *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*.

Restrictions come with sanctions directly linked to the way technology has developed and how online user interactions have proven to function nowadays. The former Directive 95/46/CE has fallen behind to being in accordance with the pace of digital environment and the way society has blended in the cyber world.

The legitimate purposes of harnessing private user data must respect the GDPR (The General Data Protection Regulation (EU) 2016/679) indifferent of the area of expertise it addresses. Commercial, political or administrative purposes are bound to address each user in a transparent manner stating the extent of processing the data provided by every person. Denial of data processing should not restrict or affect user`s access to public domains or reduce the amount of content is accessed on the account of whether permission to harness personal data is granted.

An infringement of privacy is considered necessary in a democratic society to reach a legitimate goal if it answers an essential social request, and especially if it is proportionate to the legitimate scope envisioned by the authorities to justify the limitation of privacy rights is pertinent and adequate as the European Court for Human Rights has concluded in *Coster v. United Kingdom* in 2001.

The Romanian law states that anybody has the right to have his private life respected (Article 71 the *New Romanian Civil Code*), and that nobody can be exposed to any kind of indiscretion to his intimate, personal or family life, in his

home or correspondence, without his consent or with disregard to the restrictions and limits imposed by national law or the treaties Romania has assumed. (Article 75 the *New Romanian Civil Code*). It`s also forbidden to use in any means the correspondence, manuscripts or any other personal documents, private information regarding someone without his consent or with disregard to regulations (Article 71 the *New Romanian Civil Code*).

Private life, as it is perceived by the European Human Rights Court in the 2004 *Von Hannover v. Germany* decision, is formed of elements that are directly linked to a person`s identity such as name, picture or image, physical and moral integrity. The guarantee stated by Article 8 of the Convention is mainly aimed at ensuring the development, without outside input, of each individual`s personality in relation to his keen.

Private data should not be used as currency, it is part of each person`s individuality. Like copyright, personal data can be leased but not transferred, the owner/user has the fundamental right to choose how it should be used, as this type of data persists as long as the person is alive and cannot be worn out. Despite that it has proven to be valuable merchandise for illegitimate harnessing and trade intended for generating patterns of predictive behaviour in order to micro target narratives to influence voters in political campaigns in EU states and USA the last elections.

Anybody has the right to have his dignity respected, any affliction of one`s honour or reputation is forbidden apart from given consent or outside the limits set by the Romanian law (Article 72 the *New Romanian Civil Code*). The right to have a reputation is part of private life as European Human Rights Court has settled in the 2007 *Pfeifer v. Austria* decision. One`s reputation is part if his personal and psychological identity and are the subject of one`s private life.

Personal data cannot be relinquished, but users have the right to be forgotten by the cyberspace. It doesn't mean their data disappears, it only means search engines and data base administrators will delete and not show the results related to any of the private data linked to that user.

What is interesting is that the GDPR applies also to non-members of the EU that are processing data of European residents, meaning it also changes third-party policy that is interlinked to goods and services on European market. It not only applies to policy, but it forces third-party operators to comply, due to harsh international reach of penalties imposed by the GDPR. (Rödl & Partner, 2018)

What are users experiencing in non-EU-States

India has not defined the principle of privacy in its Constitution, but has set the legal framework for Information Technology since 2000 and improved security practices and procedures by 2011 at which point sensitive personal data and information have taken an important role in this country`s revenue. So, the 2011 Rules are basically implementing the principle of responsibility for data collectors, the principle of transparency regarding the type and purpose of sensitive data collected and stored the principle of users` consent and the guarantee of data security. What Indian authorities consider sensitive information are biometric data, medical records, sexual orientation, banking history and any other piece of information that is not publicly accessible. These Rules have in fact a similar effect to what the outline of the GDPR is intended to have; only that it addresses Indian residents (Rödl & Partner, 2018).

In august 2018, the Indian authorities have drafted the framework of personal data privacy in a bill that should align to the standards of safeguarding users and support its ever-growing digital economy, by forming an independent regulatory body that should enforce data protection law and apply penalties, both to private and public sector, bearing in mind that India`s online market is only second to China`s (Balaji, 2018).

India is taking effective steps to align to European privacy policy in order to maintain trade and economic growth, proving once again that public policy is aligned to national strategy, despite other national issues and policies regarding the protection of human rights that are still a few steps back.

For comparison, the **Chinese** users have the full up-to-date legal framework to safeguard their private date hence numerous corporate and governmental data experience, but, in fact, their legal guarantees are only a part of making efficient steps toward data privacy, since Chinese illegal data transactions increase. To manifest, in April 2018 an artist called Deng Yufeng bought and included in his exhibit private data of 346,000 Chinese people (Hersey, 2018), authorities closed his art exhibition in 2 days and pursued charges.

Research on personal privacy protection in China shows that privacy content changes accordingly to background and culture, and nowadays Chinese consider that the most important personal data is the ID number, and the second is the personal phone number (See more on Zhao and Dong, 2017).

Similar to the European point of view regarding personal data, Chinese consider real names, home address and IP address an important constituent of personal data that needs to be protected by those who receive and store such

information, meaning in fact, private operators. In 2017, the Chinese Network Security Law enunciates the principles that govern data collection and the standards that should be met by any entity that collects private data. What is interesting is that the government outlined that data collection should firstly be legal, justified and necessary, then collection should be minimal, retention should be short, and usage should be within minimum scope (Udemans, 2018) the same way the European Parliament states in the GDPR.

China takes a step forward to assessing it`s citizens` private data by piloting a Social Credit System which is intended to come into force by 2020 that should be based on big data analysis technology and is intended to raise social awareness to achieve integrity as it is viewed by authorities (Botsman, 2017). The endeavour is heavily disputed, and it remains unclear how authorities will guarantee a useful toolkit to serve its citizens benefit given that it remains to be clarified in what respect the users can dispute their social score. This metadata governmental collection has taken user privacy beyond what other states are achieving through effective public policies and democratic process.

The **United States of America** data protection framework is not governed by a single principal data protection law; the protection is granted by enforcing both national and state level regulation and is achieved in different sectors by specific measures. Other states have enforced specific procedures to generally safeguard personally identifiable information of their residents. (*Data Protection 2018*) Most interestingly is that American privacy regulations are emergent from consumer protection law intended to discourage prejudicial practices, while other countries only apply policies like GDPR in order to maintain compliance and keep commercial trade on its rising course, user privacy as principle being barely emergent in national law.

A cornerstone in user privacy protection in USA was reached in 2013 when after numerous governmental surveillance disclosures, authorities have drawn a line (*Accountability and Privacy Act of 2013*) in limiting the extent of state monitoring but also harshening procedure that must be abided. The Act has been criticised as a limitation of state powers but seen by public as a guarantee of human rights in the process of preventing terrorist attacks and foreign powers` unlawful intelligence operations.

Mexico for instance has privacy as a fundamental guarantee in Constitution, powered by national personal data law governed by the same principles as those outlined by the GDPR, since Mexico has been a signatory of the United Nations Universal Declaration of Human Rights 1948, and later treaties (*International Covenant on Civil and Political Rights*, 1966 and OAS

Inter-American Convention on Human Rights, 1965) to enforce and ensure the protection of human rights.

Regarding personal privacy from a European viewpoint, in 1997 Mexico adopted Directive 95/46/EC (1995) on data protection, as part of the Economic Partnership, Political Coordination and Cooperation Agreement with the EU, and later, in 2018 adopted the Strasbourg Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981 and its Additional Protocol regarding supervisory authorities and transborder data flows (*Privacy in Mexico*, 2018).

Despite the legal framework that Mexico has accessed, authorities are criticised for not being successful in implementing effective measures to guarantee privacy as a human right, lacking a successful toolset to have public scrutiny over government surveillance. (*Privacy in Mexico*, 2018; Ahmed and Perlroth, 2017)

How users comprehend the new standard

Even though the means of communication guaranteed by internet nowadays has its benefits, users of the network cannot be effectively protected, their private life being constantly subject of unsolicited messages, images or information. The inconvenience can be reduced but not thoroughly deterred by proving the minimum digital literacy and the installation of filters. It`s not enough to identify the breach of privacy rights for an effective outcome, pre-emptive measures must be established.

Receiving unsolicited e-mails with unsolicited content is not yet a matter that can be the subject of the state`s intervention and protection if the sender cannot be identified and made responsible. For instance, the 2007 *Muscio v. Italy* decision of the European Human Rights Court has established that if the author of the breech of privacy cannot be identified, there cannot be a punishment, and art. 8 of the Convention are not violated.

How are users supposed to be prepared to interact and communicate using these new mechanisms but also keep their individuality private has come to be a balance of digital competence gained throughout work related communication and self-taught digital abilities assisted by user friendly technology.

To have a better understanding on how people perceive the rules and regulations a poll was used to measure how the public policy framework is comprehended by the people it intends to protect, and if the state policy toolset guarantees users digital literacy.

In order to appreciate the way people grasp the rules that govern the on-line sphere and to accurately measure how the public policy outline is accepted by the public they are meant to protect, we have designed the basic profile of a user that has to deal with an afflux of data and ominous threats of the digital space.

Demographics, gender or age are not criteria that should have a saying in how the user interacts on-line, since public policy has no such exceptions, the criteria we have used in studying the level of knowledge of digital space one needs in connection to the abilities one requires to successfully operate the digital space has been whether it is work related or not.

In this hypothesis it is important for our society to differentiate between the requirements of keeping up with new technology and the new facts that change the way we work and inherently influences productivity.

What we find mainly in any user is the ability to communicate and interact. That is what defines the digital space, the way people communicate. It is important to observe how this takes an important part of any person's daily on-line activity. So, our study must start from measuring the level of development of ability to successfully communicate digitally.

63% of those who answered said that at work they use frequently the on-line communication platforms, saying that it turns the work dynamics in an easier and more efficient manner.

70,4% of the respondents said that their computer skills are concurrent with what the job description usually needs for their kind of job.

64,8% of those who answered use a proprietary platform in the organisation they work.

While only 61,1% of the respondents use sometimes only digital means to interact at workplace.

From the study's perspective, the user is a person who uses a computer or a service in a network. Typically, the people who use systems and software products are not technically skilled to fully grasp how these actually function, that is why communication abilities are transferred in the digital realm as far as the user comprehends the benefits the technology he accesses has to offer, and the limits it withholds. The level of digital literacy and the efficiency of time spent doing the same operation towards the same result are directly linked.

57,4% of the respondents say that their trainings are always directly linked to their jobs specificities, while 40,7% say that only sometimes the in-house training is directed to the job description.

43,3% of those who answered the poll only sometimes take part to varied training forms, while only 7,5% always have different learning experiences.

The level of comprehension and the possibility to harness all that technology has to offer differs in direct relation to the domain the user works, indifferent of the virtual regulations imposed. Having that in mind, an important factor in this study are the means of information and self-study one uses to adapt to new technology, and whether the individual drive to study or the workplace learning tools affect the level of knowledge and skill required by today`s digitalisation. As basic reference text processing, charts and multimedia presentations were selected.

40% of those questioned answered that they seldom study the latest news regarding technology through accessing demonstrative clips, forums, professional sites or publications.

Only 46,3% sometimes work with spreadsheets, and 35,2% occasionally use multimedia presentation apps.

To clarify whether there is a link between digital skills and the career orientated trainings we must further the analysis of the source of the user`s basic digital operating knowledge and the specific capabilities required by the present in the virtual space to correctly and efficiently identify the risks of the web.

The proof of having the ability to use nowadays a network system is that the user proves to know what data security represents. One of the most outspoken ability is to avoid spam, one of the most frequent risks that can affect not only personal data integrity, but also network functions of the organisation.

Thus, the study shows that only 40,7% of those interviewed always correctly identify unsolicited electronic commercial messages for shady products or services, marking them as spam, unsubscribing, blocking, ignoring or deleting without reading.

Also, 55,6% check all the time the data asked via e-mail by checking official information or other sources of information, while 18,5% pay attention to alarming messages aimed to get one's attention towards a plausible fact, asking further dissemination.

Moreover, a valued ability to accomplish digital literacy for a user is to follow up-to-date **confidentiality** standards.

9,3% always answer to personal data requests received on e-mail from acquaintances, while 55,6% never answer.

50% always study thoroughly digital messages received from appearance to content.

After studying the legal terms 14% always consent to granting access to their personal data to the operator, 55,6% only sometimes agree to granting access, while 24,1% rarely agree, and 5,6% never consent to sharing their private data.

What changes form the user's perspective?

An increase in *digital bureaucracy*, less spamming, the same amount micro targeting for commercial purposes using more sophisticated technology, fake news persists, greater transparency of social media regarding third-party access to user private data, better liability management, compulsory independent regulator of private data management.

Conclusion

The legal framework guarantees privacy, but to put into force what the principles state, technology must answer to the standards imposed and awareness should become a strategic outline. Knowledge is gained, not a given fact.

What policy should bring to the table is attracting structural investment in digital literacy, youth educational programmes in schools and adult focused trainings, to achieve effective means of safeguarding digital privacy.

References:

1. Azam, Ahmed, Perlroth, Nicole, (2017), *Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families*, The New York Times, June 19.

2. Balaji, Sindhuja, (2018), *India Finally Has A Data Privacy Framework – What Does It Mean For Its Billion-Dollar Tech Industry?*, Forbes, August 3.

3. Botsman, Rachel, (2017), *Big data meets Big Brother as China moves to rate its citizens*, Wired UK, Retrieved 26 October.

4. Cancino, Begoña, Creel, García-Cuéllar, Aiza y Enríquez, (2018), *Privacy in Mexico: overview*, Thomson Reuters Practical Law, July 1st.

5. *Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data,* (October 24, 1995).

6. *Data Protection 2018*, International Comparative Legal Guides, June 6.

7. European Court of Human Rights, *Van der Velden v. the Netherlands*, (2006), retrieved from http://echr.ketse.com/doc/29514.05-en-20061207/view.

8. European Court of Human Rights, *Coster v. United Kingdom*, (2001) retrieved from https://swarb.co.uk/coster-v-the-united-kingdom-echr-18-jan-2001.

9. European Court of Human Rights, *Von Hannover v. Germany*, 2004, retrieved from https://www.juridice.ro/wp-content/uploads/2016/07/von-Hannover-v-Germany-ECHR-24-June-2004.pdf.

10. European Court of Human Rights, *Pfeifer v. Austria*, (2007), retrieved from https://swarb.co.uk/pfeifer-v-austria-echr-15-nov-2007.

11. European Court of Human Rights, *Muscio v. Italy*, (2007), retrieved from https://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf.

12. *Foreign Intelligence Surveillance Act* (FISA), Accountability and Privacy Act of 2013.

13. Hersey, Frank, (2018), *Artist buys and exhibits black market data of 346,000 people, invites them to visit*, Tehnode, April 10.

14. *New Romanian Civil Code*, (2014).

15. Rivas, Diego, Mantovani, Chiara, (2017), *Lawful and unlawful surveillance in Mexican democracy*, Revista Internacional de Comunicación y Desarrollo, ENSAYO, 7, 111-129, ISSN e2386-3730.

16. Rödl & Partner, *Indian Data Privacy laws and EU GDPR*, (May 24, 2018).

17. *Romanian Constitution* (1991 and 2003).

18. *Romanian Decree 212*, (1974).

19. *The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, (1981).

20. *The General Data Protection Regulation (EU)*, 2016/679.

21. *The Universal Declaration of Human Rights*, (1948).

22. *The International Covenant on Civil and Political Rights*, (1966).

23. Udemans, Cristopher, (2018), *Chinese care more about data privacy than you think, but they still need better protection,* Technode, May 15.

24. Zhao, Hui, Dong, Haoxin, (2017), *Personal Privacy Protection of China in the Era of Big Data*, Open Journal of Social Sciences, ISSN Online: 2327-5960.