TÉCNICO LISBOA

FACULDADE DE DIREITO
UNIVERSIDADE DE LISBOA

Personality Rights in the Information Society:

Citizens in the face of privacy challenges

Ricardo Miguel Ribeiro da Mata

Dissertation for the master's degree in Information Security and Law in Cyberspace

Advisor: Professor Doutor Eduardo Vera Cruz

Co-advisor: Professor Doutor Carlos Caleiro

Jury

Lisbon, October 31, 2019

Society is increasingly recognizing what are the impacts of technologies, particularly their excessive use in the lives of each of us. The ongoing technological revolution in which we live began to emerge around the year 1975, and over the years the speed of change has also increased, raising the question, when will it stop? The mind-boggling pace of transformation worries us and perplexes us, confused by a whirlwind of change that, when we begin to understand, we can no longer feel because they have already passed. We still do not have answers to many questions, but it is also true that we cannot look at the modernization of society as something exclusively negative, because that would not be true. The advantages that it has brought to our daily lives are undeniable, but with advantages they are usually disadvantages, and these are gradually being discovered, questioning whether the advantages are justified.

The fact is that we are learning to live in a new dimension of time and adaptation is occurring through successive growth crises. We live in the so-called information society and it is important to appropriate an important consequence of the meaning of this expression. Information is created from a data set, so data, as a clue or record that allows us to identify some feature of an entity or event, is at the heart of this new and dizzying world that we face. This is an important, nuclear awareness, we would say, for it is the data inherent in each of us that together shapes the present, and the way we treat it has more consequences than we might be led to think. The truth is that we do not respond as we should to our data, or at least we do not seem to give them due importance. Citizens are increasingly making their personal information publicly and globally available. With rapid technological developments and globalization, new challenges in the protection of personal data have emerged, as we must not forget that the protection of individuals with regard to the processing of personal data is a fundamental right, acquired for a long time, but now manifest another urgency. Do we live like this today in an information society where the importance of personal data is not properly perceived by citizens?

In the information and technology society in which we live today, the personality rights, and in a more modern society, the right to education, are both configurations of promotion of the human being, and knowledge is increasingly synonymous. of power but at the same time worthy survival. The importance of having a regulation that upholds these rights is important as it relates directly to the most important aspects of a person's life, with human dignity being one of the most crucial to protect. Therefore, “the existence of a general personality right is defended on the ground that, given the variety of types of violations of personality rights, the broad protection of individuals through a kind of framework right is required (Rahmenrecht) of an open nature, allowing for assumptions not previously regulated in specific legal types, something that becomes even more evident when problems related to privacy and communicative freedoms are observed.”[1]

[1] Miranda, J., Rodrigues Junior, O., Fruet, G. (2012). *Direitos da Personalidade – Principais problemas dos direitos da personalidade e estado-da-arte da matéria no direito comparado*. São Paulo: Atlas.

The right to privacy, in particular the right to intimacy of private life, is present in Portuguese law, specifically in article 80.º of the Civil Code[2]. According to José de Oliveira Ascensão, privacy comes to us in two distinct strands: "*Privacy, as opposed to advertising or the public sector of life" and "the right to reserve or the privacy of privacy, as a right of personality between others*". In the first point, the question focuses on the social sphere of human existence, extending the concept vastly, encompassing within itself various rights autonomous as personality rights, and may even say that "*privacy turns out to be the content of the personality right - almost like a mega right that exhausts the whole category*." In the second point, privacy is seen more as a defensive right, coexisting with similar ones (right to image, inviolability of home, etc.), "is the personality right, of German origin, intended to cover all defence spaces personality not specifically provided for by law".

When the topic of privacy it's mentioned, there is underlying respect, not only for people, for their ideals, but increasingly for their communications, the latter being considered a fundamental right recognized in the Charter of Fundamental Rights of the European Union. This is because the content of these electronic communications may reveal extremely sensitive information about the users covered by the communication. Similarly, metadata (descriptions of data stored in databases, or as commonly referred to as "data on data from a digital data dictionary")[3] from electronic communications can likewise reveal extremely sensitive and as categorically recognized by the ECJ (Court of Justice of the European Union).

The implementation in Portugal of the General Data Protection Regulation[4] sought to cement more solidly the issues related to the protection of personal information, using fines as its main mechanism for controlling the violation of rights. Sanctions in the less severe cases could be up to 10 million euros or 2% of annual worldwide turnover, whichever is higher and in the most severe cases the above figures will be doubled, or 20 million euros or 4% of annual worldwide turnover. Jurist Alexandre Sousa Pinheiro stated that the biggest difficulty in applying the RGPD in Portugal was the absence of national legislation, with companies and public entities seeking to escape the fines rather than seeking the correct enforcement of the requirements imposed by the regulation, something that did not help the proper functioning of it. [5] However, on 14 June 2019 the implementing law 120 / XIII on the regulation was (finally) passed in the Assembly of the Republic, which was necessary as in certain respects such

[2] Article 80.º - Direito à reserva sobre a intimidade da vida privada
1. Everyone should beware of the intimacy of private life of others.
2. The extent of the reservation is defined according to the nature of the case and the condition of the persons.

[3] de Souza, T. B., Catarino, M. E., & dos Santos, P. C. (2012). Metadados: catalogando dados na Internet. Transinformação, 9(2), p. 93.

[4] The General Data Protection Regulation (RGPD) came into force on May 25, 2018 and replaced the data protection directive and law, and there is now a single set of data protection rules for all institutions and companies active in the European Union, regardless of your location.

[5] Machado, M. (2019). RGPD. Um ano depois, os nossos dados já são privados? – Observador. Available in: https://observador.pt/2019/05/25/rgpd-um-ano-depois-os-nossos-dados-ja-sao-privados/ [Acessed june 14 of 2019].

as the age of consent for the processing of data or the fines to be imposed on private institutions needed national law.

As we consider it important to look not only at internal but also at external reality, we have decided to analyse the situation of European Union countries, such as Germany, France and the United Kingdom, as a means of comparison. We found that all of them were noticeably better prepared for the entry into force of the GDPR, with more up-to-date legislation and a society-based compliance mindset. Examples like these are needed to improve the reality in our country. Despite the introduction of these new regulations in the European Union, there is little cohesion between Member States at this level, making them somewhat isolated in combating security threats from either other countries or from internal threats. As a result, this situation leads to a noticeable differentiation between countries, with those that are more advanced and others that are somewhat behind in this matter, and, unfortunately, Portugal falls into this second range.

Looking to regulate and protect privacy on the Internet, we can mark as an event of reference, in this case in Brazil, the act known as the Marco Civil da Internet. It is a law that entered into force on June 23, 2014 and regulates the use of the internet, establishing principles and guarantees that converts the free and democratic network in Brazil, disciplining the behaviour of individuals in the virtual world. Within the European Union, the Directive on Privacy and Electronic Communications ensures "the protection of fundamental rights and freedoms, including respect for privacy, the confidentiality of communications and the protection of personal data in the electronic communications sector. It also ensures the free movement of electronic communications data, equipment and services within the Union"[6].

The issue of privacy affects us in all aspects of our lives and we often fail to have it without even realizing it. As the Internet has become part of our lives, many of us use it to replace tools that have been around in our lives for many years, such as diaries, which have been replaced by online blogs where we share our feelings, opinions, etc., so that anyone can access and give their opinion, unless of course they are placed in private modo. Failure to do so would expose private information to the Internet at serious risk of attracting unwanted actions, revealing malicious intent, and becoming more dangerous than it first appeared. Even those who put information in private can be the target of cyber-attacks (snooping or spyware, for example) that, if the computer is not well protected, can be accessed by third parties. Because of this, users should avoid giving personal information or email to suspicious advertising sites and making sure that their computer is protected with programs specifically designed to prevent such privacy violations.

[6] Directive 2002/58 / EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

The World Wide Web (WWW)[7] has infinite sets of linked documents and materials available for third parties to access. It is an inexhaustible resource of information, capable of generating knowledge, when used properly. However, several problems arise in online browsing, problems that remove the private scope in the network. The so-called clickstreams refer to the route path (sites you entered and followed links) by those who browse the WWW and contain relevance as they reveal personal interests and patterns, thus no longer just traffic data, but data from content. [8] These paths are registered in the personal computer which, associated through its IP, allows a user profile to be traced. Severely threatening to user's privacy are cookies and spyware, due to their distinctive feature, invisibility. Cookies are pieces of information that are regularly associated with a unique identifier, stored on user's computers (until 2009, before the arrival of a European Union directive, these pieces of information were stored without users' knowledge or consent) [9], which memorizes information based on its browsing behaviour. [10] Spyware is a type of malware[11] that, without the consent of the individual, collects information about your online habits, browsing history or personal information (such as credit card numbers), and generally uses the internet to pass this information on to third parties without knowledge of one's own. [12] No doubt that the tools we use have advantages in a user's daily life such as allowing an automatic login, storing preferences, keeping track of items added in the shopping carts and recording user activity, and is in this last point that the situation reverses itself and becomes more sensitive as this activity log invades the privacy of users to some extent. According to Luciano *et all*, "*All social networking and free email service providers use cookies for data collection. These cookies collect information beyond what is necessary to use these services. From these you can learn about user preferences, which can be used, for example, to target unwanted advertising and e-commerce sites offering products that meet your profile*". But according to the same authors, the "misuse of information: information disclosed can be used for brute force attacks, which consists of using an algorithm to analyse the information in order, for example, to discover passwords. , fake user profile creation, social engineering scams and answer security questions for password recovery."[13]

Some of these threats may be categorized as external threats in the sense that there is an action by an external agent at our will that deliberately violates our privacy. However, with the

---

[7] The WWW was designed by Tim Berners-Lee, a CERN researcher in Switzerland and coordinated with Robert Cailliau, whose initial purpose was file sharing.

[8] Taniguchi, D. (2009). U.S. Patent No. 7,587,486. Washington, DC: U.S. Patent and Trademark Office.

[9] Dabrowski, A., Merzdovnik, G., Ullrich, J., Sendera, G., & Weippl, E. (2019). *Measuring Cookies and Web Privacy in a Post-GDPR World. In International Conference on Passive and Active Network Measurement* (p. 258-270).

[10] Mazouchi, A., Chokhawala, A., & Kusam, A. (2019). U.S. Patent Application Nº. 15/788,466.

[11] Malware can be understood as: "a piece of code that alters the behavior of the operating system core or some applications with few security defenses without the user's consent and in such a way that it is impossible to detect these changes using documented features operating system or application" - Rutkowska, J. (2006). *Introducing stealth malware taxonomy*. COSEINC Advanced Malware Labs, 1-9, p. 2.

[12] Harkin, D., Molnar, A., & Vowles, E. (2019). *The commodification of mobile phone surveillance: An analysis of the consumer spyware industry*. Crime, Media, Culture, p. 6.

[13] SILVA, V. R. B., LUCIANO, E. M., & WIEDENHÖFT, G. C. (2016). *AMEAÇAS POTENCIAIS À PRIVACIDADE DAS ORGANIZAÇÕES CAUSADAS PELO COMPORTAMENTO INSEGURO DE USUÁRIOS: UMA ANÁLISE SEGUNDO O FAIR INFORMATION PRINCIPLES*, p. 12.

widespread dissemination of social networks, in what is commonly called Web 2.0, threats to privacy can come from the subject himself or herself, because he or she is unaware of the conditions for providing certain services that he or she subscribes to. Regarding people's image, while protected by various documents, continues to be violated in our daily lives, with video surveillance being the perfect example. The need to secure a safer society means that something must be sacrificed, and in this case, it is everyone's privacy. Similar to the Panopticon developed by the philosopher Jeremy Bentham in 1785, which consisted on a surveillance mechanism inserted in a ring-shaped building in the centre of which was a courtyard with a watchtower inserted in it, where was a prison guard, where the purpose of this tower was to provide the illusion and uncertainty to the prisoners that they were constantly being watched, when in fact they did not know if that was indeed the case because they could not see the inside of the tower due to the spotlight being constantly pointed at the cells, we are now inserted in a modern Panopticon, where instead of a prison guard watching over us, we have infinite cameras, sometimes connected to our own electronic devices that, whether we like it or not, invade our own daily privacy. Thus, the purpose of the Panopticon can be said to pass by "(…) inducing in the detainee a conscious and permanent state of visibility that ensures the authoritarian functioning of power. To make vigilance permanent in its effects (...) that the perfection of power tries to render the actuality of its exercise useless". However, with great responsibilities come great risks, and those risks are becoming more and more public. The ability of companies to control virtually all of our steps, including who we vote for in an election, such as the 2016 US elections in which Cambridge Analytica through the Facebook social network was able to influence northern-Americans voters through specific ads for each person, as they had more than 5,000 data points from all US voters, needs to be something that everyone knows, and that was one of the reasons that drove the choice of the theme in this dissertation.

Despite all the bad practices that are now starting to surface, you can't think that there are only bad points when talking about this topic. The truth is that technological advancement is allowing us to evolve, be more efficient, more productive, more educated, safer, etc., coming to the conclusion that rules must be set so that everything can continue to happen, without our own privacy being constantly violated. Starting in the cyberspace, where we spend more and more time, up until the world itself, the standards that are beginning to emerge more rigorously must be implemented. In conclusion, just as important as the above, is to make sure that the citizens are well educated and aware of the risks that their daily behaviour may pose to their privacy and, meanwhile, if the over-surveillance mechanisms by both states and organizations do not reduce and continue to regard personal information as a good/resource, the balance is very difficult to achieve.

In order not only to ascertain whether the population is really aware of the dangers inherent in their privacy, to understand whether there is a sense of alarm in most people about privacy and also to understand whether this lack of privacy is inconvenient for them, we decided to carry out a case study, where we inquired 364 persons. After analysing the results it was found, unfortunately, but predictably, that a large part of the respondents (and probably a large part of the population) are poorly informed about the lack of privacy that they suffer daily, where the responsibility, in addition to them, also lies in companies that are sometimes not transparent enough with their customers. The answers provided by

the respondents also lead to the belief that there is a sense of alarm felt by them, mainly caused by companies other than those where they work, and also by the State, giving the idea that there is a distrust felt by citizens regarding to these organs. Finally, in general, most people are indeed uncomfortable with the lack of privacy to which we are currently subjected, but with the answers given in the last question of section 3 of the questionnaire, it is clear that is not a motivation enough for many of these people to attend a online course where they would possibly clarify most of their doubts and how they might change certain uncomfortable privacy situations.

In conclusion, the results presented in this case study suggest that Internet users in Portugal should carry out an insight into the importance of preserving the privacy of their personal information and the revaluation of their behaviour (especially online) and how they expose their information in their daily personal life online. It should be emphasized that capacity building and awareness raising should be carried out, especially for young people. Not only that, but a strong investment in the formal education system must emerge, introducing the topic of security and privacy into the curriculum of at least one subject area, which would necessarily mean properly educating teachers.

Bibliographic References

Dabrowski, A., Merzdovnik, G., Ullrich, J., Sendera, G., & Weippl, E. (2019). Measuring Cookies and Web Privacy in a Post-GDPR World. In International Conference on Passive and Active Network Measurement (p. 258-270).

de Souza, T. B., Catarino, M. E., & dos Santos, P. C. (2012). Metadados: catalogando dados na Internet. Transinformação, 9(2).

Harkin, D., Molnar, A., & Vowles, E. (2019). The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. Crime, Media, Culture.

Machado, M. (2019). RGPD. Um ano depois, os nossos dados já são privados? – Observador. Available in: https://observador.pt/2019/05/25/rgpd-um-ano-depois-os-nossos-dados-ja-sao-privados/ [Acessed june 14 of 2019].

Mazouchi, A., Chokhawala, A., & Kusam, A. (2019). U.S. Patent Application Nº. 15/788,466.

Miranda, J., Rodrigues Junior, O., Fruet, G. (2012). Direitos da Personalidade – Principais problemas dos direitos da personalidade e estado-da-arte da matéria no direito comparado. São Paulo: Atlas.

SILVA, V. R. B., LUCIANO, E. M., & WIEDENHÖFT, G. C. (2016). AMEAÇAS POTENCIAIS À PRIVACIDADE DAS ORGANIZAÇÕES CAUSADAS PELO COMPORTAMENTO INSEGURO DE USUÁRIOS: UMA ANÁLISE SEGUNDO O FAIR INFORMATION PRINCIPLES.

Taniguchi, D. (2009). U.S. Patent No. 7,587,486. Washington, DC: U.S. Patent and Trademark Office.