From the Borderless Digital Chambers to Prison's Four Walls After Committing Personal Data Unlawful Acts

Larisa-Mădălina MUNTEANU
Data Protection Lawyer and Deputy Data Protection Officer, JS Information Governance Ltd, Peterborough, the United Kingdom
larisa@js-ig.com

Abstract

This paper represents a concise comparative presentation of how and why can imprisonment be a penalty in different legal systems when committing cybercrimes that affect personal data. Yet, since personal data is closely linked to cybersecurity (especially in cases of non-compliance with regulatory standards), the subject matter herein will focus on the subsequent relationship between personal data and cybercrimes, but from a peculiar perspective - how impactful unlawful acts can be so as to result in criminal convictions. It relies, therefore, on a symbiosis of acknowledging where personal data sits in the cybercrimes' ecosystem and applying this to the most threatening cases identified by global regulators. In this context, the current research is contingent on mirroring the major legal models worldwide, based on which these offences are sanctioned with imprisonment. It is utterly thought-provoking to analyse how the contrasting legal provisions are driven by a common goal: preventing cybercrimes or, as the case may be, minimising their consequences. All these differences have, essentially, homogenous values at a foundational level. Particularly, that foundational level is the research core of this paper.

Index terms: cybercrimes, electronic data, global legal systems, imprisonment, personal data protection

1. Introduction

Once upon a time, we used to write essays about how flying cars will be the most innovative development in the world, how robots will efficiently assist humans in daily tasks and how cities will be increasingly computerized. I was myself one of those essay makers. Contrastingly, now I wonder if these ideas and expectations were actually something worth waiting for. Nowadays, we might as well discuss about how life without computers would not be that deplorable.

Having these thoughts as premise, this paper will focus on the emergence of one of the negative consequences stemming from digitalisation - cybercrimes. However, the presentation will be shaped in the context of personal data, as the modern (non?) material assets. In this context, a different facet of cybercrimes will be shaped. This refers to regulatory frameworks implemented by regulators as preventive and corrective mechanisms, focusing on the most serious penalty - imprisonment.

Within the underlying research, it was easily concluded that electronic personal data is exposed to an extremely high risk when discussing cybercrimes. The reasons will be presented in the following sections. Also, this paper will put the basis of an illustrative perspective of personal data cybercrimes, in the light of different international legal systems. The purpose of this study is not to create a comprehensive list of how states around the world decide to 'discipline' individuals that do not comply with data protection laws, but rather to expand on how legislators act when serious unlawful

acts are committed. This is why, there might be cases when it would have been interesting to mention additional legal systems, but, for space and time concerns, limitations were necessary. Nonetheless, I am looking forward to preparing a more extended version of this study in the future.

Moreover, this paper will hopefully put an end to the existing misconception that the data protection laws prescribe only fines (and in secluded cases, warnings). This thesis is plainly wrong for a number of reasons, but the main one is that sometimes, imprisonment is the third possible penalty, as expanded in the following chapters.

2. Legal dimensions of cybercrimes

To begin with, it is essential to understand what cybercrimes are, before thoroughly analysing particular hypotheses of identifying them. According to the United Nations Office on Drugs and Crime, 'There is no international definition of cybercrime nor of cyberattacks'. Yet, the typical acts can be classified as it follows: 'i) offences against the confidentiality, integrity and availability of computer data and systems; ii) computer-related offences; iii) content-related offences; iv) offences related to infringements of copyright and related rights' [1]. Given the topic of this paper, the first category is the one of interest.

From a judicial perspective, the Directive on attacks against information systems pinpoints the statutory foundational level, on which it is built: the Convention on Cybercrime of the Council of Europe (the Budapest Convention) [2], labelling it 'the legal framework of reference for combating cybercrime, including attacks against information systems' [3]. Thus, it is worth underlining this Convention, which is also the first international framework with regards to regulating cybercrimes. However, since its preamble explains the underlying necessity of this treaty as to 'deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data', a strong connection with personal data protection emerges. Yet, when discussing personal data safeguarding in the European space, the instrument that will most frequently be put forward and weighed up is the General Data Protection Regulation (hereinafter GDPR) [4].

Nonetheless, these two instruments do closely overlap: the Budapest Convention intends to sanction cybercrimes, whilst the GDPR acts as risk-based approach guidance. At the same time, it was concluded that 'The points of overlap between the Budapest Convention and GDPR is that cybercrime will necessarily be conducted in abusing data in one way or another' [5, p. 70]. Yet, although they both regulate on collecting, disclosing data, the Convention covers more than personal data. Therefore, it is difficult to conclude which of the legal frameworks has more narrow practical applicability: the Convention safeguards computer data and traffic data (including, but not limited to personal data) [2, Ch. 1, Art. 1], whilst the GDPR protects personal data (including, but not limited to electronic data). Furthermore, the EU enforced a more specific instrument, for ensuring privacy and personal data protection are respected exclusively in digital networks: the E-Privacy Directive [6].

Similarly, the Digital Markets Act is expected to be enacted soon, imposing obligations on the core digital platforms in order to respect the GDPR, the E-Privacy Directive, the cybersecurity legislation, along with consumer protection and product safety [7, Art. 7 (1)]. By building the rationale in this way, it became more striking that these puzzle pieces are more than intertwined - they depend on each other for allowing extensive digital protection to online users. Also, the necessity of these instruments is more incontestable than ever, since the data produced digitally is expected to grow spectacularly to 175 zettabytes by 2025 [8]. Correspondingly, 'If cybercrime was a country in this context, it would have been the world's 13th largest economy measured by Gross Domestic Product (…)' [5, p. 64].

However, it is important not to glorify (cyber) security to an excessive as balance is the key. Believing otherwise would just lead to social and regulatory chaos, whilst people might get 'blind' by the obsessive illusion of exhaustively regulating the cyberspace, which is impossible. Eventually, just as Dwight D. Eisenhower stated in 1961, 'We will bankrupt ourselves in the vain search for absolute security' [9]. Although this principle was born from a political context which is inapplicable now, the essence must still be considered: pure and unlimited security is not a realistically achievable goal. Nevertheless, it is important to have flexible regulators that can keep up the pace with perpetrators' strategies and tools, especially in digital realms.

Even if personal data might not be the ending, it might be the means: cybercrimes might not focus on personal data, but rather financial data. However, perpetrators need personal data to gain access to the financial data. Another perspective is that if they have personal data, they can easily make assumptions as for sign-in credentials on relevant platforms.

3. Data breaches and other security incidents as cybercrimes

To continue, after understanding the meaning and limits of cybercrimes, the current section intends to expand and apply this foundation. Thus, as a principle, stealing information and unlawfully accessing or using data can easily become a main target for worldwide Criminal Laws. The most frequent such cases illustrate incidents concerning corporate confidential data or financial data. However, since personal data is briefly defined as information [4, Art. 4], how frequent is personal data a threatened actor? Usually, according to the UK Information Commissioner's Office (hereinafter ICO), cyber incidents are caused by human error [10] and can be quite frequent, affecting 'four in ten businesses' [11].

Nonetheless, it was concluded for a while now that when addressing '(…) broad cybercrimes, privacy and data protection become a value to be balanced against prosecuting the crime' [12, p. 68]. Consequently, impersonation is already prohibited by Criminal Laws (especially the frequent cases of using false IDs in order to obtain unfair advantages, even if punished under different names). Then, one may question, what is the difference between using a false ID in order to access the confidential area of a company and using false IDs online, for entering their confidential servers or databases of a company? It seems that more often than not, the offences having a component of personal data are 'taken' online nowadays - and online is very accessible, but also very dangerous. However, since personal data can be both in printed and electronic form, the framework should be a common one, as long as not otherwise mentioned.

On the other hand, unlawful acts concerning personal data are currently covered by data protection laws. That means they are not usually directly perceived as having a connection with the Criminal Law. Nonetheless, Recital 149 of the GDPR allows Member States 'to lay down the rules on criminal penalties for infringements of this Regulation', including with regards to the obligations stemming from enforcement of the GDPR at national level. Also, Art. 84 highlights the main requirement imposed on national legislators - the additional penalties to administrative fines must be 'effective, proportionate and dissuasive'.

In practice, in specific jurisdictions, because of the impactful effects produced, imprisonment was deemed as the suitable penalty. Consequently, a thin line connects the personal data concept with the Criminal Law realms. Even if more and more legal systems choose to 'activate' criminal liability for serious cases of non-compliance in personal data protection, it becomes more interesting to discuss which states included imprisonment as a penalty and in which conditions.

The applications will be discussed in the following section, focusing on the circumstances that can lead to an individual being subject to imprisonment. The chief reasons for this approach depend on the thought-provoking rationale lawmakers used in order to decide in favour of including this sanction in national regulations. The way this mechanism works is more than debatable, blooming on

a dichotomy of minimising the consequences and reshaping the individual: '(…) the aim of imprisonment is to reconstitute the prisoner's spatiotemporal world without causing avoidable collateral damage' and 'cannot be divorced from the characteristics of the societies in which they take root' [13, p. 46].

4. Models of global legal systems

Although a connection between imprisonment and data protection non-compliance seems to be a far reality for most readers, the truth is that legal systems do actually fancy this approach. However, the regulations are not homogenously structured worldwide. As a consequence, the following paragraphs will guide the audience towards observing, conceptualising and incorporating the major global models of how imprisonment is chosen as a suitable penalty for the most severe non-compliance acts in personal data protection. The three subchapters suggested below are following a logical order, based on the emphasis regulators placed on the system of penalties, meaning the legal consistency and precision of relevant regulations. Some countries do recognise the necessity of imprisonment as a punitive measure in certain impactful scenarios explicitly in their data protection laws related laws, whilst the others rely on legal interpretation, with varying degrees.

4.1. Explicitly included in the national data protection laws

In Germany, some acts referring to personal data might trigger criminal liability, if committed 'deliberately and without authorisation' - for example, transferring data to a third party or making it accessible for commercial purposes could lead to imprisonment up to three years. On the other hand, the intent aspect is altered if the processing is carried out without authorisation or by fraudulent acquiring of data, since imprisonment (up to two years) is an option only if the intent was to obtain payment in return or to enrich oneself or harm someone [14]. In reality, since many online perpetrators do carry out such illicit acts in exchange of money, the practical applicability of this legal provision is indisputable.

Italy is another eloquent example. The Personal Data Protection Code prescribes some cases in which imprisonment is the penalty prescribed by the law, yet the maximum period is 3 years. Should an individual provide false statements or 'submit forged records (…) in a proceeding before the Garante and/or in the course of inquiries' [15, Sect. 168], they might be subject to such conviction. The rationale for this might be the indubitable proof of contempt for the Italy's National Data Protection Authority. However, the minimum imprisonment period that can be set on an offender is 6 months - this is relevant for non-complying with the rules on traffic data, location data or unsolicited communications [15, Sect. 167 (1)]. In this context, it can be easily inferred that traffic data and location data have a special regime in comparison with other types of information. Should this mean the Italian legislator included them in a *de facto special category* that is worth implementing higher levels of data protection? The conclusion lays on a rather gray area. Based on the following paragraph [15, Sect. 167 (2)], it comes to light that disregarding the requirements established for sensitive data [15, Sect. 26] results in a less lenient sanction - imprisonment from 1 to 3 years under the condition that harm is caused. Consequently, traffic data and location data are treated differently (with more strictness) by the Italian Code, but that does not mean they become sensitive data or they supersede the 'privileged' regime of sensitive data.

In South Africa, the Protection of Personal Information Act [16], particular offences might result in imprisonment for up to 10 years. What is even more striking is that fines can be imposed simultaneously. So, whilst other systems apply the 'ne bis in idem' principle prohibiting such outcomes, South Africa explicitly allows the opposite. Nonetheless, it is important to note that the right not to be tried or punished twice is encompassed in the European Convention on Human Rights (ECHR) [17], explaining why South Africa followed a parallel approach. To exemplify, this is the

case if the concerned party 'hinders, obstructs or unlawfully influences the Regulator (…)' [16, Sect. 100] or 'fails to comply with an enforcement notice' [16, Sect. 103 (1)]. It can be concluded once again that cybercriminals might face serious consequences caused by their thoughtlessness in relation with Data Protection Authorities, highlighted by the Italian system as well.

4.2. Explicitly included in related laws

Contrastingly, in the United States, the main peculiarity is the inexistence of a unique data protection law. In reality, the US relies on different regulations and levels - both statal and federal. However, the Data Security and Breach Notification Act 2017 holds valuable information supporting this paper. It is prescribed that if security breaches are 'intentionally and willfully' concealed, the individual concerned is subject to a fine or imprisonment up to 5 years, or both, under the condition the damages have an economic nature of at least $1,000 [18].

In other states, personal data protection laws coexist with sector specific laws. In the United Kingdom, the specific laws on personal data protection (Data Protection Act 2018 and UK General Data Protection Regulation) do not establish any legal grounds permitting imprisonment in cases of non-compliance. However, ancillary statutory instruments do - within the Computer Misuse Act 1990, for example. Herein, Sect. 3ZA(6) prescribes that unauthorised acts causing or creating a significant risk or serious material damage can be convicted on indictment 'to imprisonment for a term not exceeding 14 years, or to a fine, or to both'. From a legal perspective, it is at least interesting to discuss how the 'ne bis in idem' principle is practically applied in this case, just as in the South Africa instance. The only reasonable solution would be to impose an administrative fine in addition to imprisonment, otherwise the ECHR's protection would not be relevant - as highlighted in Prina v Romania [19].

Other relevant prohibited criminal act is the unauthorised access with intent to commit or facilitate commission of further offences (s2), clarifying that in the UK system, cybercrimes' preparatory acts are explicitly punished as well. In practice, the Supervisory Authority (ICO), had issued the first prison sentence in 2018, relying on s1 of the Computer Misuse Act 1990, when the concerned individual used a password of someone else in order to access company's records, including personal data, and continued to do so even after working for another company [20]. Subsequently, the second conviction in ICO's history happened in 2021, for unauthorised access and unlawful transfers of personal data [21].

These cases could be referred to as a benchmark for the topic of this paper - they doubtlessly shape how the unlawful obtaining of personal data (prohibited by specific data protection legislation) was practically merged with more technical legislation (countering unauthorised acts and practices against computers). In this context, it becomes crystal clear that personal data assets are one of the most frequent targets when discussing cybercrimes.

On the other hand, the Data Protection Law in France [22] recently amended the Defense Code with regards to processing information about the military status of individuals and established the main sanctions in case of non-complying with the legal requirements set out in these provisions. These can be a fine or up to three years imprisonment, depending on the particular disregarded obligation (e.g. not informing the relevant minister of the processing, allowing access to third parties in prohibited instances etc.). Moreover, the French Criminal Code encompasses other cases in which overlooking personal data protection standards results in punitive effects, countering cybercrimes. In chapter VI, section V, imprisonment is one of the main penalties - e.g. for five years, as an alternative to a € 300,000 fine, if special categories of data are processed without data subject's consent [23, Art. 226-19] or if the collection of data was carried out using 'fraudulent, unfair or unlawful means' [23, Art. 226-18]. Furthermore, cybercriminals that make illicit transfers of personal data outside the European Union might be subject to these penalties too [23, Art. 226-22-1].

Also, Turkey is one of the most exceptional cases in terms of legal structure, from a data protection standpoint. The national Data Protection Law] establishes the main data protection principles, procedures, complaints, cases of administrative fines, but refers to the Criminal Code when it comes to 'crimes' [24, Ch. 5, Art. 17]. Consequently, according to these provisions, the toughest sanction is imprisonment from one to four years for unlawfully delivering, publishing or acquiring data to another person [25, Art. 136], whilst the opposite is imprisonment from six months to one year for failing to destroy data subject to a legal requirement [25, Art. 138]. However, an essentially interesting aspect is to be noted: committing any of these offences with regards to special categories of personal data does not constitute an aggravating circumstance since they follow the same legal regime [25, Art. 135 (2)], but taking advantage of one's position might be. To continue, the imprisonment period is increased by half if in the particular case, the law was broken 'by a public officer or due influence based on public office' or 'by exploiting the advantages of a performed profession and art' [25, Art. 137].

4.3. Implicitly included in related laws

In Romania, the National data protection law does not encompass imprisonment as a sanction. This fact is confirmed by the law establishing the Data Protection Authority, which states its powers rely on imposing fines and warnings. However, the Criminal Code [26] might be of interest in this context. In the Special Part, Chapter V of Title VII, called 'Offenses against security and integrity of computer systems and data', imprisonment is the principal penalty to be imposed (yet, in some cases, alternatively with fines). Since the legislator referred in these cases to computer data (in relation with unauthorised access or transfer, illegal interception, alteration etc.), it becomes crucial to acknowledge the exact meaning of this concept. Can personal data be included in computer data? Based on Art. 181 (2) of the General Part, the answer is positive and stands by the literal interpretation, easily applied in this case - shortly, computer data includes any data that can be processed by means of a computer system. In practice, this means that affecting electronic personal data in such circumstances lays the foundation of discussing about cybercrimes.

On the other hand, Art. 302 of the Criminal Code prescribes the cases of violating the privacy of correspondence, briefly defined as the unauthorised opening, stealing, destroying, keeping or revealing of correspondence addressed to another individual. In practice, there are numerous cases in which correspondence contains personal data (let alone that it already includes the contact details of both the sender and receiver) - it might even include photos, which are biometric data, and consequently included in the special categories of personal data. In such cases, it is crucial to understand that the effects, based on the spirit of the GDPR, are much more threatening for the data subject's rights and freedoms. Therefore, to conclude, the Romanian system has no explicit provisions for allowing individuals being sentenced with imprisonment for breaching their data protection obligation. Yet, this might be possible when personal data is structured in an electronic format, and when one of the conditions of one of the above offences are met.

Similarly, Brazil implemented the same system. The National Data Protection Law does not empower the National Authority to sentence individuals to imprisonment for such non-compliance acts, but the Criminal Code might be applied in this case [27]. Exactly as in the Romanian legal framework, the Criminal Code encompasses crimes committed against computer systems and more specific, information systems. One interesting aspect about the Brazilian legislation is that recently, a very specific punishable conduct is the 'fraud committed through social networks, telephone contacts, fraudulent e-mails, or any other similar fraudulent means by using information provided by the victim or by an error caused by a third party', subject to up to eight years of imprisonment and a fine. Aggravating forms include using a server outside of the country or having 'elderly or vulnerable' victims[27, Art. 171].

5. Conclusions

All in all, in the 'Era of Seeking for Privacy', personal data has become one of our most valuable assets. It was highlighted within this study that cybercrimes are closely linked to personal data, but this hypothesis remains valid primarily with regards to electronic personal data.

On the other hand, active involvement has been noticed from both private and public bodies, in a global movement towards protecting personal data and combating non-compliance acts and perpetrators. In my opinion, it seems that protecting electronic personal data is gaining more attention than ever.

However, offences were portrayed differently by worldwide regulators, yet discrepancies do depend on socio-cultural, political and even economic values. This resulted in a uniform perspective in some countries, proving the need to legislate on these matters for enforcing punitive and restorative justice. Contrastingly, the way penalties were regulated, structured and imposed was fluctuating. This paper planned to emphasise some of the legal systems around the world, classified from a data protection perspective, with the purpose of delimitating what regulators consider to be 'serious' offences. It can easily be inferred by any individual that although cybercrimes and electronic personal data are cohabitating in borderless realms, penalties are real and impactful.

To conclude, this brief written presentation was not intended to cover each structure legal systems use when sentencing individuals to imprisonment for personal data related cybercrimes, but to extend the reader's perspectives on the severity of this phenomenon. This is not a comprehensive study - it is rather food for thought, addressed to any reader interested in the legal dimensions of cybercrimes when personal data is at stake.

References

[1]. Global Programme on Cybercrime, UNODC. Accessed Mar. 18, 2022. [Online]. Available: https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.

[2]. Convention on Cybercrime, opened for signature 23 November 2001, ETS No 185 (entered into force 1 July 2004).

[3]. Directive 2013/40/EU of the European Parliament and of The Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L218/8 Recital 15.

[4]. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[5]. D. Wicki-Birchler, "The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime?," Int. Cybersecurity. Law Rev., vol. 1, no. 1-2, Sept 2020, doi: 10.1365/s43439-020-00012-5.

[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) [2002] OJ L 201/37.

[7]. Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) COM(2020) 842 final.

[8]. T. Coughlin, "175 zettabytes by 2025." Forbes.com. https://www.forbes.com/sites/tomcoughlin/2018/11/27/175-zettabytes-by-2025/?sh=3e648f075459 (Accessed Mar. 21, 2022).

[9]. J. N. Las Vegas, "LETTER: Eisenhower, spending and communism," in Las Vegas Review Journal, Sept. 2021. Accessed Mar. 12, 2022. [Online]. Available: https://www.reviewjournal.com/opinion/letters/letter-eisenhower-spending-and-communism-2438000/.

[10]. Kaspersky, "Human Factor in Corporate Cybersecurity," 2019. Accessed Mar. 28, 2022. [Online]. Available: https://media.kaspersky.com/en/enterprise-security/KL_Human%20factor_main%20threats_datasheet.pdf.

[11]. ICO, "Cyber Security Breaches Survey 2021," 2021. Accessed Mar. 28, 2022. [Online]. Available: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021.

[12]. M. G. Porcedda, "Data Protection and the Prevention of Cybercrime: The EU as an area of security?." 2012. Distributed by EUI Working Papers LAW 2012/25 [Online]. Available: http://hdl.handle.net/1814/23296.

[13]. I. O'Donnell, "The aims of imprisonment," in Handbook on Prisons, Y. Jewkes, B. Crewe, J. Bennett, Eds., London, U.K.: Routledge, 2016 pp. 39-54.

[14]. Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097), as last amended by Article 12 of the Act of 20 November 2019 (Federal Law Gazette I, p. 1626), Part 2, Ch. 5. Sect. 42.

[15]. Personal Data Protection Code containing provisions to adapt the national legislation to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 2021.

[16]. Act No. 4 Of 2013, Protection of Personal Information Act (POPIA).

[17]. Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR), Protocol no. 7, Art. 4.

[18]. U.S. Senate, 115th Congress, 1st session (2017, Nov. 30). S.2179, Data Security and Breach Notification Act, Sect. 5 § 1041.

[19]. Prina v Romania (2020) ECHR 267.

[20]. J. Clark, S. Qureshi and A. Greaves, "UK: First prison sentence following ICO prosecution." DLA Piper. https://blogs.dlapiper.com/privacymatters/uk-first-prison-sentence-following-ico-prosecution/ (Accessed Mar. 29, 2022).

[21]. F. Fellowes and K. Barnes, "ICO Utilises the Computer Misuse Act to Impose Tougher Penalties for Unauthorised Access to Data." Squire Patton Boggs. https://www.consumerprivacyworld.com/2021/02/ico-utilises-the-computer-misuse-act-to-impose-tougher-penalties-for-unauthorised-access-to-data/ (Accessed Mar. 30, 2022).

[22]. Law n°2018-493 of 20 June 2018, on the protection of personal data.

[23]. French Criminal Code, 2005.

[24]. Law on the Protection of Personal Data No. 6698, 2016.

[25]. Turkish Criminal Code - Law Nr. 5237, 2004.

[26]. Law on the Criminal Code no. 286, 2009.

[27]. Decree-Law nº 2,848 of December 7th, 1940 (Brazilian Criminal Code).