
CYBERLAW
by CIJIC

CYBERLAW by CIJIC

EDIÇÃO N.º VIII – SETEMBRO DE 2019

REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA


CYBERLAW
by CIJIC

CYBERLAW by CIJIC

ISSN 2183-729

NOTAS DO EDITOR:

Nesta nova edição da revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa, dada a pertença do CIJIC ao grupo do Network of Centers (https://networkofcenters.net/center/cyberlaw-research-centre-university-lisbon-school-law-cijic), a obrigação identitária desta comunidade, persuade-nos a publicar artigos em inglês. Traremos, portanto, duas investigações em anglo-saxónico.

Na oportunidade presente da publicação desta VIII Edição e dos actos legislativos nacionais em curso, foi nossa opção trazer uma visão jurídica sobre o poder, eventualmente, manipulativo da democracia através das redes sociais.

O contexto é o da eleição presidencial de 2018, no Brasil, mas o modo como se desenvolve, desde uma engenharia social mais dissimulada a uma difusão de *fake news* ou *deep fakes*, permitem utilizar tais distorção de forma globalizada. Sendo certo que carece de maior investigação o real efeito da *realidade* das redes sociais *versus* o do "*quotidiano não digitalizado*" e o resultado concreto disto em sede de apuramento final dos resultados de eleições livres e universais, parece já possível concluir que, mesmo ante esta condicionante ainda não determinada, a realidade democrática pode, efectivamente, ser *hackeavel*.

Não obstante, por princípio, a clarificação dos conceitos de *fake news* e *deep fakes*, deveria afastar-se do radical "notícia" que lhe dá a alma. Porque uma notícia corresponde a um acto jornalístico, exercício com tutela constitucional, que conclui um dado conteúdo factual, relatando acontecimentos de interesse geral da comunidade com

o maior grau de objectividade possível. Uma notícia identifica-se pela clareza, simplicidade, exatidão, e pelo bom uso da língua em que é escrita. Compreende contraditório, ou a possibilidade deste, suporta-se em fontes credíveis. Há todo um ónus ético e deontológico que sopesa uma notícia assinada por um jornalista. Toda esta súmula é uma notícia. Comentário, mesmo televisivo, liberdade de opinião, todos os outros "*fenómenos*", não se identificam com este radical conceptual. Logo, porque continuamos a insistir em querer colar uma qualquer liberdade opinativa ao conceito de "notícia"?

Não vos soa ridículo o exercício de contínuo *fact-check* a exercícios de liberdade de opinião? Desde quando é que mentira foi legalmente proibida? Mas, pelo contrário, uma notícia que veicule um facto falacioso, de cariz subjectivo, não é fortemente sancionável? Desde logo pelos poderes de regulação, pela sindicância da própria classe, pelo público?

Será assim tão difícil perceber as diferenças?

Noutro plano, em efeméride do décimo aniversário da Lei do Cibercrime portuguesa, a Lei n.º 109/2009, de 15 de Setembro, olhamos para a perspectiva da aptidão do enquadramento legal, num contexto nada fácil, de obtenção de resultados eficazes em tempos, da acção *contra-legem versus* investigação, demasiado assíncronos. Qual a razão que explica a falta de enquadramento legal nacional para o agente (digital) encoberto, quando dezenas de outras polícias de investigação, congéneres, já o fazem?

Se há disciplina onde a soberania das fronteiras físicas acabou é no digital. Outrossim, pela fragilidade dos "muros" digitais e das deficiências do enquadramento jurídico-penal nacional, abordaremos ainda o fenómeno do *Ransomware*. Dez anos volvidos da Lei do Cibercrime, e em apologia à vanguarda em que já estivemos nos idos do início da década de 90 do século passado, impõe-se no presente, em 2019, o revisitar a especialidade da lei do cibercrime. O contexto presente de *leaks* de índole variada e processos mais ou menos mediáticos, reclamam prudência. A digitalização do Estado, por outro lado, impõem mudanças assertivas. Ademais, quer a falta da criminalização do roubo de identidade digital[1], quer a complexidade jurídico-penal do

1 Atente-se por exemplo no Considerando (14) da Directiva: "(…) *A adoção de medidas eficazes contra a usurpação de identidade e outras infrações relacionadas com a identidade constitui outro elemento importante de uma abordagem integrada contra a cibercriminalidade. A necessidade de intervenção da*

Ransomware, quer a própria transposição da Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013 (esgotado o prazo de transposição no ano de 2015), quer a protecção do Estado digital (e não só) reivindicam melhores ferramentas, desde logo legais, que bem que poderiam servir de impulso necessário ao dormente legislador nacional.

Por fim, tema que não sai das agendas, o Regulamento geral de protecção de dados. Desta vez, as fricções que a ferramenta *blockchain*, cada vez mais usada no contexto das relações entre particulares e organizações, compreende face ao RGPD mas, e também, a melhor consecução dos objectivos proclamados pelo RGPD que esta ferramenta pode ajudar a alcançar.

Por fim, mas antecipando o futuro, atendendo ao propósito identitário da revista, passaremos nas próximas edições a publicar artigos de investigação dos alunos do Mestrado em Segurança da Informação e Direito do Ciberespaço, trabalhos estes desenvolvidos nas cadeiras que frequentarem.

Resta-me, neste final, agradecer a todos quantos contribuíram para mais uma edição da Revista, pelo esforço e pelo trabalho, enereçando, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, um reconhecido:

- Muito Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

Boas leituras.

Lisboa, FDUL, 29 de Setembro de 2019

Nuno Teixeira Castro

União contra este tipo de comportamento criminoso poderá também ser ponderada no contexto da avaliação da necessidade de um instrumento transversal e abrangente da União."

CYBERLAW

by CIJIC

DOUTRINA

CYBERLAW by CIJIC

THE PUBLIC SPHERE (FORGED) IN THE ERA OF FAKE NEWS AND BUBBLE FILTERS: THE BRAZILIAN EXPERIENCE OF 2018

EDUARDO MAGRANI [1]

&

RENAN MEDEIROS DE OLIVEIRA [2]

1 Doctor and Master in Constitutional Law from the Pontifical Catholic University of Rio de Janeiro (PUC-Rio) and Senior Fellow at Humboldt University in Berlin, Alexander von Humboldt Institute for Internet and Society. Coordinator of the Institute of Technology and Society of Rio de Janeiro (ITS Rio). Research Associate at Law Schools Global League and member of the Global Network of Internet & Society Research Centers (NoC). Professor of the disciplines of Law and Technology and Intellectual Property at renowned universities such as FGV, IBMEC and PUC-Rio. Lawyer active in the fields of Digital Rights, Corporate Law and Intellectual Property. Author of several books and articles in the area of Law and Technology and Intellectual Property. Contact: https:linktr.ee/Eduardo_magrani

2 Master's degree in Public Law and Bachelor of Law from the University of the State of Rio de Janeiro (UERJ). Post-graduate in Public Law from the Pontifical Catholic University of Minas Gerais (PUC Minas). Researcher at the Diversity Program at Getulio Vargas Foundation (FGV) School of Law and at the Fundamental Rights Clinic of the Faculty of Law of UERJ - UERJ Rights Clinic. Renan was an intern at The Center for Technology and Society at FGV School of Law. Contact: renanmedeirosdeoliveira@gmail.com

ABSTRACT

In this article we intend to explore, through the bibliographical review and the study of poll of voter intentions in Brazil, a little of the new technological phenomena that, together, affect the way in which the citizen forms his opinion about the everyday facts significant for public life, in general, the electoral process and the candidates, in a discerning way. Firstly, we take into account a brief approach to the theoretical framework in which we are based to think of a communicative, rational public sphere and in which the ideal situation of speech is sought. Secondly, we deal with the fake news - which is about false news that desires to influence the way the population looks at a particular candidate - and deep fakes - which have a similar goal but act by altering the reality in a more profound way. Finally, we approach how the algorithms, especially the use of bots, are acting in order to create a forged public sphere which does not match the real desire and the real need of individuals. In addition, we deal with how the thinking of individuals is being distorted in the filter bubble scenario, which potentializes the effects of the phenomena studied in the preceding items. Throughout the development of this study and through the hypothetical-deductive method, we will seek to demonstrate that the new technologies have a great potential of impact on the electoral will, although this potential has not yet been explored in all its extension. It walks into a scenario where the electoral process is hackable.

Keywords: Conected democracy; Fake News; Bots; Filter bubble scenario; Deep fakes.

RESUMO

No presente artigo pretendemos explorar, através da revisão bibliográfica e do estudo de pesquisas de intenção de votos, um pouco dos novos fenômenos tecnológicos que, juntos, impactam a forma como o cidadão forma sua convicção acerca dos fatos cotidianos importantes para a vida pública, de modo geral, e do processo eleitoral e dos candidatos, de modo particular. Em primeiro lugar, fazemos uma breve abordagem do arcabouço teórico em que nos baseamos para pensar numa esfera pública comunicativa, racional e na qual se busca a situação ideal de fala. Em seguida, tratamos das *fake news* – que se tratam de notícias falsas que buscam influenciar a forma como a população olha para determinado candidato – e das *deep fakes* – as quais têm objetivo similar, mas agem por meio da alteração da realidade de forma mais profunda. Por fim, abordamos como os algoritmos, sobretudo o uso de bots, estão agindo de modo a criar uma esfera pública forjada, que não condiz com o real desejo e com a real necessidade dos indivíduos. Além disso, tratamos de como o pensamento dos indivíduos está sendo distorcido no cenário das *filter bubble*, que potencializam os efeitos dos fenômenos estudados nos itens precedentes. Buscaremos demonstrar, ao longo do desenvolvimento deste estudo e através do método hipotético-dedutivo, que as novas tecnologias possuem um grande potencial de impacto na vontade eleitoral, por mais que esse potencial ainda não tenha sido explorado em toda sua extensão. Caminha-se para um cenário em que o processo eleitoral é *hackeável*.

Palavras-chave: Democracia conectada; *Fake News*; *Bots*; Filtros-bolha; *Deep fakes*.

1. INTRODUCTION

Fake news has previously demonstrated itself to be a powerful influencer in the electoral process. At the moment of forming his opinion, the voter suffers the impact of news whose truthfulness is not investigated, creating a judgment in relation to the candidates and the democratic process based on false news. It is not possible to affirm the exact dimension exercised by the fake news in the electoral process, but it is a fact that they exercise some influence.

The probable harmfulness of fake news is exponentiated when we consider how the new technologies are being used together. Deep fakes, algorithms, the filter bubble, among others, define the way you view reality, affecting aspects of life that go beyond elections. Questioning the status quo and veracity of incidents is something positive and essential in a democracy. However, it is necessary to have minimal consensus on facts, especially those of public interest. The great volume of news that puts in doubt the way things have been given in reality decreases the ability of people to differentiate the real from the invented.[1] It is indispensable that basic ethical standards are respected in order to ensure a minimally healthy democratic environment.

The scenario aggravates when one takes into consideration that traditional media, especially television, is losing space and confidence. The citizen does not believe in all that is said on TV anymore, believing the contents to be biased and out of context.[2] Television, in addition, exercises a significant role, but it must be taken into account that this role is being downgraded and space is being given to the internet, focusing on social networks. However, although the Internet is a source of tireless content and allows the search for information on the part of the user, the phenomenon that was perceived as filter bubble creates obstacles to a healthy and democratically desirable online dialogical environment.

In this article, we attempt to explore, a little of the phenomena that, together, impact the way

1 Natalia Viana and Carolina Zanatta, 'Deep Fakes are Threatening on the Horizon, But They Are Not Yet a Weapon for Elections, Says Expert' *The Public* (16 October 2018) <https://apublica.org/2018/10/deep-fakes-sao-ameaca-no-horizonte-mas-ainda-nao-sao-arma-para-eleicoes-diz-especialista> accessed 25 October 2018 (Viana and Zanatta).

2 The data demonstrated a clear generational distinction in relation to sources of obtaining information: the higher the age, the greater the use of television as the main means of communication. Up to 24 years of age, more than half of young people use the Internet as their main means. See the data of the Brazilian Media Survey 2016 (*Pesquisa de Media*, 2016) <https://bit.ly/2YH6udr> accessed 29 October 2016.

in which the citizen forms his opinion regarding the everyday facts important to public life and the electoral process and candidates. Firstly, we briefly outline the approach to the theoretical framework in which we think about a communicative, rational public sphere and in which the ideal situation of speech is sought. Secondly, we deal with *fake news* and *deep fakes*. In a few words, fake news is that news that seeks to affect the way the population looks at a given candidate. Deep fakes have a similar objective, they purely act by altering reality in a deeper way. Finally, we approach how the algorithms, specifically the use of bots, are acting in order to create a forged public sphere which does not match the real desire and the real need of individuals. In addition, we deal with how the thinking of individuals is being distorted in the filter bubble scenario, which potentializes the effects of the phenomena studied in the preceding items.

For the purposes sought here, we will broadly rely on the literature review on *fake news*, deep fakes, bots and filter bubble and on the impact of these phenomena in the elections and in the formation of the opinion of individuals. We will also be resorting to the survey of the intent of votes. Thus, we will seek to demonstrate, throughout the development of this study and through the hypothetical-deductive method, that the new technologies have a great potential for impact on the electoral will, although this potential has not yet been explored fully. It envisages a scenario where the electoral process is hackable.

2. BRIEF THEORETICAL NOTE: THE VIRTUAL PUBLIC SPHERE

One of the aims of this study is to point out the need for minimum ethical standards in the use of new technologies and mechanisms to circumvent the abuses arising from the utilitarian perspective, preventing the use of a person as a means and not as an end in itself. With this, we want to avert forms of manipulation of real profiles or the use of bots in order to create priorities forged in the public agenda. We can think of the most appropriate ethical perspective to deal with technology in a context in which democratic procedures and actions are related to the complex world of data and constant man-machine interaction in which we live. It is therefore essential to be ethical and moral not only on purpose but also to the entire procedure and range of actions.

For this,[3] we understand that it is necessary to take into account the complete and complex theoretical perspective of Jürgen Habermas, which allows us to think about the advancement of this new world of data in a dialogical and participatory way to achieve more legitimate and consensual regulatory proposals.

The German thinker, born in 1929, experienced in post-war Germany, with the Nuremberg trials, the depth of the moral and political failure of Germany in the realm of National Socialism.[4] Habermas stood out in the academic world by analyzing the development of the bourgeois public sphere from its origins in the halls of the eighteenth century, until its transformation through the influence of media directed by capital. [5]

For Habermas, the legitimacy of norms and the political system in contemporary capitalist Western capitalist societies depends on the acceptance of norms by citizens.[6] This occurs through successive attempts at justification in which each citizen must freely bind his will to the content of the norm through a rational and dialogical process of argumentation, that is, of reflection and conviction.[7]

---

3 The main concepts and formulations of Jürgen Habermas and their relation with the internet platforms can be checked in a study by Eduardo Magrani, *Connected Democracy: The Internet as a Tool for Political-Democratic Engagement* (Juruá 2014) (Magrani).

4 James Bohman and William Rehg., 'Jürgen Habermas' *The Stanford Encyclopedia of Philosophy* (2007) <https://plato.stanford.edu/entries/habermas/> accessed 29 July 2019.

5 With the publication in 1962 of his habilitation, Jürgen Habermas, *Strukturwandel der Öffentlichkeit (Structural Transformation of the Public Sphere)* (English edn, Polity 1989).

6 Jürgen Habermas. *Law and Democracy: Between Facticity and Validity*, vol 2 (2nd edn, Tempo Brasileiro 2003) 16 (Habermas).

7 Joshua Cohen, 'Deliberation and Democratic Legitimacy' in James Bohman and William Rehg (eds), *Deliberative Democracy: Essays on Reason and Politics* (MIT Press 1997) 29.

In this type of society, the public sphere is precisely understood as the set of spaces that allow the occurrence of dialogical processes of communication, of articulation of opinions and reflective reconstructions of values, moral and normative dispositions that guide social coexistence. It is in the public sphere that the different constitutive groups of a multiple and diverse society share arguments, formulate consensus and construct common problems and solutions.[8]

The public sphere of Habermas comprises a zone of interchange between, on the one hand, the system – depicted as the world of work, guided by the logic of money and power, as an instrumental world of strategic action, noncommunicative, oriented by the market and bureaucracy[9] - and, on the other hand, the public and private spaces of the world of life - characterized as the world of interaction between people, which are organized communicatively through the ordinary language, enabling communicative action without a strategic action, oriented only to intersubjective understanding that ideally leads to agreement or leads to consensus.[10]

Habermas excelled in the academic world by evaluating the development of the bourgeois public sphere from its origins in the halls of the eighteenth century to its transformation through the influence of media directed by capital. The colonization would be the result of the meddling of politics and economy in the world of life, responsible for the reduction of citizenship and the transformation of the citizens into clients of social welfare services, that being the hallmark of modernity. In this scenario, the power of economic capital and politics invades the world of life destructively. According to Habermas, systemic intervention has a destructive impact on cultural reproduction, social integration and socialization as components of the world of life.[11]

While the author has not specifically and deliberately addressed the topic of the internet, we advocate the prospect of understanding digital platforms as abstract public spheres with great communicative and democratic potential.[12] We find in the digital spaces a public sphere in which individuals communicate regularly, through discussion forums, social networks, or

8 Magrani (n 5).
9 Jürgen Habermas. *The Theory of Communicative Action*, vol 2 (Beacon Press 1987) 113-197; Craig Calhoun (ed), *Habermas and the Public Sphere* (MIT Press 1992) 1-51.
10 Habermas, *Law and Democracy* (n 8) 107.
11 Although Habermas predicts that there is no complete shielding of the life-world of systemic logic, he believes that this logic can be nullified by the very dynamics of the world of life, based on communicative action.
12 For an in-depth treatment of this defense, cf. Magrani (n 5) 25ff; The Habermasian theory alone does not sufficiently help us to deepen the possible solutions to these problems, since it was thought mainly to measure and induce the behavior of the rational and dialogic human agent that interacts in the public sphere. However, it serves as an excellent paradigm for analyzing the real possibilities of building a dialogue and speech scenario in the *online* context.

platforms for exchanging messages that nearly approach the conception of the public sphere drawn by Habermas on a smaller scale.

However, with the advancement of the most recent digital technologies, we have also followed the transformation of these connected spaces, and it is possible to envisage a possible reduction in their communicative democratic potential.

Today we observe the predominance in the connected spheres of profitable business models based on algorithmic filtration with the objective of conducting microtargeting practices, profiling, among others, directing the sale of products and services in a way Optimized for e-consumers. These current practices are based on the use to a large extent of the personal data of users and generate the aggravation of the effect called "Filter bubble", having harmful effects on democracy and braking the enthusiasm about the democratic role of the Internet as a public sphere for contemporary societies. In the following items, we considered some of these mechanisms and their ethical implications for the democratic context as a whole and for the elections in a specific way.

3. FAKE NEWS AND DEEP FAKES: DO THEY REALITY EXIST?

The fake news calls, fake news created for the purpose of misinforming, are hitting users with greater precision than expected. The type of content sent can also take into account the personal profile of those who will read the news in order to cause more direct impact, which is delivered by the microtargeting technique.

The fact is increasingly apparent that data produced by users on the Internet is being collected in some way by third parties. Not only personal data, but also what they read, research, and specifically, their consumption habits. At the same time, the Internet enables the massive uptake of these data if it is processing on a large scale. This large volume of data – structured, semi-structured or unstructured[13] – forms the big data, technology that allows people to know more and more individuals, and can even identify them personally by observing their habits, preferences and desires.

The richness of this information is such that it becomes inevitable to question how users allow such collection by consenting, for example, with the terms of use of websites and applications. It happens, firstly, that the terms of use are usually extremely technical and unintelligible to the general population, which makes the given consent not be completely conscious. Secondly, the performance of the companies itself is not always made transparently, that is, often the real purpose destined to the data is hidden from the users.[14]

With this and the increasing amount of data produced daily, the management of this information by third parties is worrisome. This is because big data goes far beyond a tangle of data: it is essentially relational. As individuals do not have control of their own personal data, it can be said that it belongs to those who collect them, creating a harmful vertical relationship.

Such technology opens an opportunity that has not gone unnoticed in the market. With this volume of data, there is a possibility of automatic personalization of content on digital platforms, including directing this filtering through targeted advertising, made possible through the tracking of cookies and by processes of retargeting, or programmatic media (behavioural re-targeting).

Companies observe the inputs generated by these data to guide their market policy in order

13 Julia Lane and others (eds), *Privacy, Big Data and the Public Good: Frameworks for Engagement* (CUP 2014).
14About the terms of use on the internet, cf. Eduardo Magrani and others, *Terms of Service and Human Rights*: *An Analysis of Online Platform Contracts* (Revan 2016).

to achieve the desires and habits of consumers, through techniques such as tracking, profiling and targeting. This is done according to the behavioural trends analyzed, which leads to a targeting, therefore, of the market choices through the creation of targets. Today, we observe the predominance of the connected spheres of profitable business models based on algorithmic filtration in order to direct the sale of products and services optimally to e-consumers.

The microtargeting technique is a digital strategy for establishing the target audience through the collection of data from this audience so that the company can thoroughly know the profile in question. The strategy is done on top of a database assembled with information such as age, gender, hobbies, behaviour, among others. In principle, *microtargeting* was used in advertising marketing for the enhancement of products and services. Now there is talk of political marketing as it assists candidates to define a niche of specific voters by mapping possible supporters.

One of the advantages of microtargeting is to allow anticipating results that can be achieved at the end of the advertising or political project, delivering savings of time and money on the part of the agents, since their focus will be qualitative over what the targets actually want or need, dispensing with random attempts. These current practices, therefore, are guided by the use to a large extent of user data through big data that, in addition to making dishonest use of personal information, it can also generate political consequences, such as the worsening of the effect called "Filter bubble", harmful to the democratic role of the Internet as a public sphere, and the potentialization of false news.[15]

On this political-democratic context, some examples can help you comprehend how microtargeting is used to leverage false news. The paradigmatic case is that of the 2016 elections in the United States, hard impacted by the fake news. It is stated that the rumours largely assumed a negative content regarding Democratic candidate Hillary Clinton, in contrast to encouragement for the conduct of Republican Donald Trump. Fact is that, in 2016, 33 of the 50 false news on Facebook dealt with the political context lived in the United States.[16]

---

15 On the relationship between fake news and elections, it is recommended to read the open letter advocated by the Coalition of Rights in the Network group, which provides guidelines on the subject. Open letter from civil society representatives from Latin America and the Caribbean on concerns about the fake news and elections, Coalition of Rights on the Network, 'Fake News and Elections' (*Rights on the Net*, 2017) <https://direitosnarede.org.br/p/carta-aberta-americalatinaecaribe-igf2017/> accessed 29 October 2017.

16 Craig Silverman, 'Here Are 50 of the Biggest Fake News Hits on Facebook From 2016' (*BuzzFeed News*, 30 December 2016) <https://www.buzzfeednews.com/article/craigsilverman/top-fake-news-of-2016#.nl712lkw2> accessed 29 October 2018; 'There are 7 Types of Fake News. Do You Know Them All?' (*Magic Web Design*, 19 March 2018) <https://www.magicwebdesign.com.br/blog/internet/existem-7-tipos-fake-news-voce-conhece-todos/> accessed 29 October 2018.

Some false news has had such repercussions that they have run the world, like, for instance, that Pope Francis – and, therefore, the Roman Catholic Church – supported Donald Trump's candidacy, which would give him even greater support from the layers conservatives of American society. The rumour was disclaimed only when the Vatican spokesman made a public announcement saying that the pope never manifested such support and, neither, intends to take political positions.

Countries like Russia have also influenced the American electoral process. Among the rumours scattered, an army of "Russian trolls" published news that Hillary Clinton would be involved with satanic ritual practices. One of the narrative lines affirmed, upon alleged e-mails leaked between Hillary and his campaign manager, John Podas, that they participated in rituals with a priestess who adored the demon. It was, however, a performance of the artist Marina Abramovic on Spirit cooking, which was challenged in one of the hacked emails of the campaign.[17] Later, U.S. intelligence discovered that e-mails were hacked into an operation orchestrated by the Kremlin.[18]

However, a recent case that became emblematic and, in fact, aroused attention on how microtargeting can be used to disseminate false news, is that of the company Cambridge Analytica, appointed as one of the main vectors of viralization of fake news, as well as Donald Trump's victory in the elections.

The case begins with the creation of an application that ran on Facebook, thisisyourdigitallife, created by Cambridge Analytica scholar, Dr Aleksandr Kogan, active at the University of Cambridge, with the objective of developing academic research. For this, the app collected private information from the profiles of 270,000 users, with their consent, which until then was allowed and was in accordance with the terms of use of Facebook. It happens that, in 2015, the social network in question was validated that Cambridge Analytica had shared the data collected with a third party, the company Eunoia Technologies, which aimed at commercial purposes, in disagreement with the terms of use of the platform.[19] In this way, Facebook demanded that the information provided to third parties be destroyed, only thereafter

17 Benjamin Lee, 'Marina Abramović Mention in Podesta Emails Sparks Accusations of Satanism' *The Guardian* (4 November 2016) <https://www.theguardian.com/artanddesign/2016/nov/04/marina-abramovic-podesta-clinton-emails-satanism-accusations> accessed 29 October 2018.
18 'How Russia-Linked Hackers Stole the Democrats' Emails and Destabilized Hillary Clinton's Campaign' *ABC News* (5 November 2017) <https://www.abc.net.au/news/2017-11-04/how-russians-hacked-democrats-and-clinton-campaign-emails/9118834> accessed 29 October 2018.
19 'Privacidade No Facebook: o que aprender com a Cambridge Analytica' (*Irisbh*, 19 March 2018) <http://irisbh.com.br/privacidade-no-facebook-cambridge-analytica/> accessed 28 October 2018.

it was discovered that Cambridge Analytica and other companies did not eliminate the information, which is why they would be suspended from operating on the platform from that moment on. At this point, nonetheless, the data of about 50 million Facebook users had already been compromised.

The scandal only came to the public in March 2018, when Christopher Wylie, who worked to get data from users on Facebook and passed it on to the company Cambridge Analytica (who was contracted internationally by several politicians in electoral times), issued Statements to the press, revealing that the profiles were gathered for the purposes of political manipulation in the connected public sphere.[20]

This case raises attention to some important factors. The App—thisisyourdigitallife functioned as a personality test that also financially rewarded those who agreed to participate. This represents a strong appeal to the user of social networks, who tends to want to satiate the curiosity of the results of these tests, which have become so common, even more by the possibility of earning some profit from it. In a masked manner, therefore, the company managed to collect a large amount of data, in a way that was consented to the use of a distinct purpose.

The secret purpose, it was later found out, was to collect data to chart voter profiles in order to use them for electoral marketing. This is nothing more than a microtargeting strategy, making use of the technology of the *big data* to attain a more refined material, suitable for producing even more precise results.

The company spent about US $1 million in data collection to send messages directed to specific voters, manipulating their political opinion through an algorithm that could analyze individual profiles and determine personality traits linked to the online behavior of the voter, as well as his feelings and fears, directed the content of sociopolitical manipulation based on these components. Therefore, an esteemed range of data collected by Cambridge Analytica was sold to political parties to, from an analysis, produce fake news capable of reaching the voter in what is most importante to him/her. That is, corroborating or attacking their more rooted positions, with the objective of dissuading them, with the certainty of success.

With this, it is essential to be clear that, in the final analysis, the big data is the individual in

20 Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach' *The Guardian* (17 March 2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> accessed 29 April 2017.

all its complexity and, therefore, one must have a critical conscience and think possibilities to regain control over personal data.[21] It is necessary to address judicial and extrajudicial forms of data protection, of the accountability of companies that carry out such activity. And, above all, to build a conscious use of the platforms in the users, so that they do not so easily give away their information in false exchanges of benefit, that turn against them in a way so painful for the society and the democracy in general.

Similar to the Donald Trump campaign in 2016, the Jair Bolsonaro campaign in 2018 in Brazil used several fake news to promote the candidate. The strategy became public when the press disclosed the existence of contracts of the candidate with private companies totalling about 12 million reais through which companies bought packets of message shots against the opposite party (PT) in WhatsApp, which comprised of the disclosure of false news.[22] The candidate also counted on the participation of groups of volunteer people who organized the creation and circulation of fake news.[23] The false news with the greatest repercussion during the elections concerned the "Gay Kit " and the fraud in the polls, and other news that circulated less dealt with the accusation that Fernando Haddad (PT) would be paedophile and that Jair Bolsonaro (PSL) would want to change the patroness of Brazil.[24]

Another way to come to subjugate the electorate is deep fake. The technologies already allow the recording of audios with imitation almost similar to the voice of people and the editing of videos in which the face of an individual who has never been in the situation appears as a participant. If in the daily scenario of non-public people, this is already extremely harmful to honour and image, this risk grows exponentially when we talk about public people. Audios and edited videos can be used, for instance, to defame the image of a certain candidate to an electoral position.

---

21 Eduardo Magrani and Renan Medeiros de Oliveira, 'We are Big Data: New technologies and Personal Data Management' (2018) 5 CyberLaw 10-33 <http://www.cijic.org/publicacao/> accessed 29 July, 2019.

22 Pedro Ortellado, 'Bias on the Internet Does Not Seem to Be Caused by "Bubbles"' (*Folha de São Paulo*, 2018) <https://www1.folha.uol.com.br/colunas/pablo-ortellado/2018/02/polarizacao-na-internet-nao-parece-ser-causada-pelas-bolhas.shtml> accessed 29 October 2018; Patricia Campos Mello, 'Entrepreneurs Campaign Against the PT by WhatsApp' (*Folha de São Paulo*, 18 October 2018) <https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml> acessed 29 October 2018.

23 Mariana Simões, 'Pro-Bolsonaro Groups on WhatsApp Orchestrate Fake news and Personal Attacks on the Internet, Research Says' *El País* (24 October 2018) <https://brasil.elpais.com/brasil/2018/10/23/politica/1540304695_112075.html?id_externo_rsoc=FB_BR_CM&fbclid=IwAR05Mw9zXzmjDbYv5OkjAm1hVipWBURMCPyiOORIaxSsy_qNxEjzrpHKxfQ> accessed 29 October 2018.

24 '"Voter Fraud" and "Gay Kit" Have a Greater Impact than Other Fake Twitter, Facebook and Youtube News' (*FGV DAPP*, 1 Novemeber 2018) <https://observa2018.com.br/posts/fraude-nas-urnas-e-kit-gay-tem-maior-impacto-que-outras-noticias-falsas-em-twitter-facebook-e-youtube/> accessed 29 October 2018.

A recent case illustrates this possibility. On October 23, 2018, a video was circulated on the internet in which, supposedly, the candidate for governor of the state of São Paulo, João Doria (PSDB), appeared in intimate scenes with women. Five days after the second round of elections, the circulation of a video in this sense is enormously damaging to the image of the applicant, especially when it is considered that Doria is a defender of the traditional family. The then-candidate filed for investigation in Electoral Court. Initially, the investigations in relation to the video denoted that it would be assembly or simulation: expert report stated that the face of the candidate would have been wrongly inserted into the video, putting him in a situation in which he did not participate.[25] Subsequently, a new report punctuated the truthfulness of the video.[26]

This is a definitive case of deep fakes. Moreover, reality itself is called into question, and what is true or false is no longer known. This creates a mental confusion in the electorate, which happens to believe in one side without any solid ground. All being questionable, the human desire for an answer grasps at any clue of truthfulness - whether this clue is supported by some proven fact or only in self-deception.[27]

After the video was released, the voting intentions surveys showed some variation in the percentage points of each candidate. According to Datafolha's survey, on October 25 2018, Doria had 52% of votes, while on the 27th of that month it had fallen to 49%.[28] Considering the intensity of the campaigns in the days immediately preceding the elections and the profusion of information that is disclosed, we can not affirm that the video was directly responsible for this fall. In addition, the first forensic report disclosed indicated that the video would be an assembly or simulation, which may have caused more doubts in the voter. Fact is that the disclosure of this deep fake, accompanied by expert reports that did not indicate a single solution, was not enough to prevent the victory of the candidate, who won with 51.77% of the valid votes. Note, however, that we can affirm that the video was an important factor to be faced in the final moments of the campaign. In the current context, citizens are aware that there is an indiscriminate disclosure of *fake news*, so that they can consider, without any

25 Sérgio Quintella, 'Expertise Reveals Report on Intimate Video Attributed to João Doria' *Veja São Paulo* (24 October 2018) <https://vejasp.abril.com.br/blog/poder-sp/pericia-aponta-montagem-em-video-intimo-atribuido-a-joao-doria/> accessed 29 October 2018.

26 Redação Pragmatismo, 'Intimate video of João Doria is true, new report points out' (*Pragmatismo Político*, 26 October 2018) <https://www.pragmatismopolitico.com.br/2018/10/video-intimo-joao-doria-verdadeiro-pericia.html> accessed 29 October 2018.

27 Eduardo Gianetti, *Lies We Live By: The Art of Self-deception* (Companhia das Letras 2005)

28 Gabriela Fujita, 'SP: Datafolha shows France with 51% and Doria, 49%; Ibope brings 50% for each' *UOL* (Sao Paulo, 27 October 2018) <https://noticias.uol.com.br/politica/eleicoes/2018/noticias/2018/10/27/datafolha-ibope-sp-doria-franca.htm> accessed 29 October 2018.

evidence in any of the senses, that the disclosure of the video was merely a ruse of the opposition to discredit the adversary. Thus, they ignore whether the video was indeed true or false and cling to the beliefs already formed - which are often based on *fake news*.

In this context,[29] there are bills that seek to criminalize the disclosure of false facts during the electoral year, such as House Bill No. 9973/2018, 10292/2018, 9931/2018 and 9532/2018. The Senate Bill No. 246/2018 is broader and seeks to insert in the Civil Framework of the Internet "measures to combat the disclosure of fake content or offensive Internet applications." In addition, there are groups intended to accomplish fact-checking. But in a scenario where everything is questionable, who will check the truthfulness of the check on reality? The profusion of true and false information could lead to an "infocalypse," as Aviv Ovadya[30] warns. That is why we affirm above that it is essential to guarantee a minimum level of consensus on reality and a respect for fundamental ethical principles.

The impacts of this manipulation of the public sphere go far beyond the elections. In the long term, it may be that the elaboration of public policy-making is based on a forged popular will, generating state expenditures that do not meet the real needs of citizens. Moreover, the constant legitimacy of the actions of politicians can be forged, even if unattractive public policies are put into practice. In the following item, we made some considerations about the filter bubble and its impact on the opinion formation of individuals and the configuration of the public sphere.

29 An exhaustive enumeration and detailed presentation of all bills on the subject would require its own study and would go beyond the limits of this article.

30 Aviv Ovadya, 'What's Worse Than Fake News? The Distortion Of Reality Itself' [2018] 35(2) New Perspectives Quarterly 43-45.

4. THE PUBLIC SPHERE FORGED BY ALGORITHMS AND THE PERSONAL CONVICTION IN THE FILTER BUBBLE AGE [31]

Filter Bubble[32] can be defined as a set of data produced by all the algorithmic mechanisms used to make an invisible edition aimed at the customization of online navigation. In other words, it is a kind of personification of the contents of the network, made by certain companies like Google, through its search engines, and social networks, like Facebook, among several other platforms and providers. It is then formed, from the navigation characteristics of each person, a particular online universe, conditioning their navigation. This is done by tracking various information, including the user's location and cookie registration.[33]

With these techniques that generate the bubble filters, the internet would be transforming into a space in which is shown what is thought to be of interest to us. Thus, we are almost always hidden from what we really want or eventually need to see. Thus, it can be said that the filter bubble is paternalistic and prejudicial to the debate and the formation of consensus in the connected public sphere, being possible even to question its constitutionality, since it can suggest restrictions to fundamental rights, like access to information, freedom of expression, as well as the autonomy of individuals.[34]

Filtering has emerged as a necessity and is often considered welcome, generating a great deal of comfort for the user, who quickly and efficiently finds, in most cases, the information or any other content that he wants to access. This is Netflix's business model, for instance, which allows the user to have at his disposal a collection of movies based solely on his profile through the suggestion of personalized titles and filters, in order to improve his experience.

Though, beyond convenience, the problem lies in the form and in the excess of filtering, both by the companies and by the individuals themselves, who, unconsciously, restrict themselves and move away from contradictory perspectives, impoverishing, the value of the debate in the virtual public sphere. Consequently, bubble filters limit users to what they wish

---

31 Some of the considerations made in this chapter were explored in Eduardo Magrani, 'The Internet of Things: Privacy and Ethics in the Age of Hyperconnectivity' (Pontifical Catholic University of Rio de Janeiro 2018); *See also* Magrani, *Connected Democracy* (n 5).

32 Eli Pariser, *The Filter Bubble: What the Internet is Hiding from You* (Penguin Press 2011).

33 As Tim Wu notes in Tim Wu. *The Master Switch*: *The Rise and Fall of Information Empire* (Vintage 2011), "Cookies are, in a nutshell, access data that consist of the "digital footprints" left when passing through and manifesting through online environments."

34A peremptory statement in this direction would require further study, so that the specific approach of this point would go beyond the limits of this study.

(or would like) according to, most often, an algorithmic prediction.[35] This creates a problem in accessing the information that should be seen to enrich the democratic debate.

Furthermore, from another perspective, the internet user, when navigating the most well-known sites, is today the target of a torrent of targeted advertising that signifies the commercial interest behind this filtering and personalization mechanism.

The internet is plastic and alterable, and the reality that we involuntarily become hostage to the algorithms that insert us into these bubbles has been seen as one of the most drastic but subtle changes because they are often indistinguishable. The filter bubble's premise is that the user does not unintentionally decide what appears to him within the bubble, nor does he have access to what is left out.

The information curation executed by traditional media, including offline media, already materializes the concept of content filtering by choosing and separating a series of information. Habermas, as well as other Frankfurt School theorists, such as Adorno and Horkheimer,[36] was in advance attentive to the traditional media force and its effect on modern democracy.[37] Nevertheless, internet platforms are often deficient of sufficient transparency in their informational and algorithmic clipping, giving consumers a false idea that information has a neutral and free flow. In addition, algorithm filtering in online environments allows for a degree of customization and targeting on a much larger scale,[38] which tends to accelerate with the coming of the Internet of Things,[39] given that with more and more intelligent devices connected around us, we will have even more personal data being collected, stored and treated.

In the light of the above, the idea that Internet infrastructure as a public sphere has the potential to allow the discussions to be strong enough to reach different segments and different interest groups, replicating through the various networks of people who make up society, may be an increasingly distant reality. This is due to the fact that the expressions are often restricted to the same network of people with common interests and communication channels easily negotiated by the platform holders. The conclusion of this is the broadening of communication fragmentation and the polarization of public debate.[40]

---

35 Evgeny Morozov, *To Save Everything, Click Here*: *The Folly of Technological Solutionism* (Public Affairs 2013)
36 Rolf Wiggershaus and others, *The Frankfurt School: Its History, Theories, and Political Significance* (MIT Press 1995).
37 Habermas, *Law and Democracy* (n 8) 99.
38 Magrani, *Connected Democracy* (n 5).
39 Cf. Eduardo Magrani, *The Internet of Things* (FGV Editora 2018).
40 As Cass Sunstein notes in Cass Sunstein, *Republic.com 2.0* (Princeton University Press 2009) and Cass

In a Habermasian view of legitimizing the political-democratic system, this scenario is unacceptable, since the minimally free communication flow must be preserved in the public space, allowing all those who may be reached to have a voice and participate in an increasingly direct way in decisions, whether appropriate to their private or political context in the public sphere. A quintessential example of this is the case of Cambridge Analytica, depicted in the previous item.

With the gain of greater sophistication and free-will of the technologies, our interaction with these agents will become more and more complementary and complex, bringing to the surface, still, a greater capacity of manoeuvring our thought and behaviour.

We must add to this—as a negative thing—the reality, that we often do not know how the algorithms of the intelligent objects we use and the virtual spaces in which we interact—work.[41] Each time these new nonhuman agents produce effects on our actions or even make significant decisions in our place through the customization of the information that is offered to us.[42]

Broadly speaking, decision-making and communicative democratic interaction today are undergoing an intensified transformation, as they suffer the intermediation and agency of non-human agents, such as robots or algorithms equipped with some degree of artificial intelligence. These elements are influencing our interaction and our discourse with the capacity to produce significant political-democratic material effects, so they should be better comprehended for regulatory purposes.

In political discussions, robots have been used across the party spectrum not only to win followers but likewise to conduct attacks on opponents and forge discussions. They manipulate debates, produce and circulate false news, and influence public opinion by posting and

---

Sunstein, *Republic.com* (Princeton University Press 2001), bubble filters would be a serious risk to the potential of the connected public sphere due to the lack of contact with dissenting opinions and the polarization of discourses leading to radicalism. This would be a problem with trends not to its resolution, but to its aggravation, from the sophistication of content customization algorithms.

41 Frank Pasquale in Frank Pasquale, *The Black Box Society*: *The Secret Algorithms that Control Money and Informatio*n (Harvard University Press 2015) criticizes this situation by treating today's algorithms as black boxes and shedding light on the effects of this on a society guided in several areas by algorithmic data and decisions.

42 In 2017, in Wisconsin in the US, a judge awarded a six-year prison sentence, taking into account not only the defendant's criminal record, but also his COMPAS score (Correctional Offender Management Profiling for Alternative Sanctions), which is a tool algorithm that aims to predict the risk of recidivism of an individual. The score suggested that the defendant had a high risk of committing another crime; so his sentence was six years. The defendant appealed the ruling, arguing that the judge's use of the predictive algorithm in his sentencing decision violated due process and is based on the opacity of the algorithms. Cf. Adam Liptak, 'Sent to Prison by a Software Program's Secret Algorithms' *The New York Times* (1 May 2017) <https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html?mtrref=www.google.com.br&gwh=B3F9140AAAB1DACDFCE11CBD55F4DB8F&gwt=pay> accessed 29 October 2017. The case went to the United States Supreme Court, which denied the writ of certiorari, refusing to consider the case.

replicating messages on a prominent scale. Many *bots*[43] have reproduced hashtags on Twitter[44] and Facebook[45] that gain eminence by massaging automated posts in order to strangle sudden debates on a particular topic.

Firstly, automated accounts can even confer positively to some aspects of life on social networks. The chatbots,[46] for instance, streamline customer service and, in some cases, even help consumers process their requests and get more information. Nevertheless, an increasing number of robots act with spiteful purposes in the public sphere. The social bots (social robots) are accounts controlled by software, which artificially generate content and establish interactions with non-robots. They attempt to imitate human behaviour and to pass as such in order to interfere in legitimate and voluntary debates and produce forged discussions.[47]

The growth of robot-led action thereupon represents a real danger to public debate, representing hazards to democracy itself, interfering with the process of consensus building in the public sphere, and in choosing representatives and government agendas.[48] For no other

43 The term Bot, short for Robot (or Internet bot or web robot), is a software application that aims to provide an automated service to perform generally predetermined tasks. They mimic human behavior and are being used in politics and elections to influence opinion in digital networks, such as social networking platforms, instant messaging, or news sites. A conceptualization of the term can be found in Clara Velasco and Roney Sundays, 'What is a Web Robot and How Can it Influence the Debate in Networks? Experts Explain' (*G1*, 2017) <https://g1.globo.com/economia/tecnologia/noticia/o-que-e-um-robo-na-web-e-como-ele-pode-influenciar-o-debate-nas-redes-especialistas-explicam.ghtml> accessed 29 October 2017.

44 According to the PEGABOT project, from the Institute of Technology and Society of Rio de Janeiro (ITS Rio) and the Institute of Equity & Technology, "[u] m Twitter Bot is an account controlled by an algorithm or script, usually used to perform tasks for example, retweet content containing particular keywords, respond to new followers, and send direct messages to new followers. Twitter Bots complex blogs can participate in online chatting and, in some cases, behave very much like human behavior. Bot accounts make up 9 percent to 15% percent of all active Twitter accounts, but more in-depth studies indicate that this percentage may be even greater because of the difficulty of identifying complex bots. Twitter bots are generally not created with malicious intent; they are often used to improve online interaction or service delivery by companies, governments and other organizations, so it's important to separate good bots from bad bots. <https://pegabot.com.br> accessed 27 October 2018.

45 Robots are easier to spread on Twitter than on Facebook for a variety of reasons. An explanation on the subject can be found in Marco Aurélio Ruediger, 'Robots, Social Networks and Politics in Brazil: Study on Illegitimate Interference in the Public Debate on the Web, Risks to Democracy and the Electoral Process of 2018' (*FGV DAPP*, 2018) <http://dapp.fgv.br/en/robots-social-networks-politics-fgv-dapp-study-points-illegitimate-interference-public-debate-web/> accessed 29 July 2019 (Ruediger).

46 Institute of Technology and Equity, 'Experts Explain How the Robot can Influence the Debate in Networks' (*Medium*, 15 December 2017) <https://medium.com/@tecnoequidade/especialistas-explicam-como-o-robô-pode-influenciar-o-debate-nas-redes-3a844f911849> accessed 29 October 2017.

47 Ruediger (n 47).

48 Bots account for more than 50% of the internet traffic around the world. Some bots are intended, for example, to require accountability of politicians, to root out causes for gender equality, or to help organize the (many) daily tasks of their users. Already other bots are aimed at spreading lies to influence conversations in the public sphere, a phenomenon that since 2014 has been gaining global scale. These bots are out there and hardly anyone knows how they work, who develops them and who they are funded. To illustrate this point, recent research has shown that the repercussion of the cancellation of the Queermuseu event, thoroughly commented on in the national press, has been inflated by robots on the internet. Of the more than 700 thousand tweets analyzed, 8,69% were triggered by bots, hampering public discussion. "While the decision to cancel exposure has taken other factors into account, it is possible to say that bot action has impacted on the way the debate was conducted, and its practical

rationale, there are bills in Brazil at the federal level to discourage the use and contracting of *bots* for electoral objectives, such as Senate Bill No. 413/2017, which strives to criminalize "the supply, hiring or the use of an automated tool that simulates or can be confused with a natural person to generate messages or other interactions, through the Internet or other communication networks, in order to impact the political debate or to interfere in the electoral process."

Confirming the thesis of risk to democracy, the Directorate for Public Policy Analysis (DAPP) of the FGV disclosed illegitimate interference in the online debate through the use of the 2018[49] and 2014 elections[50] and in public debates in general.[51] Scheduled accounts for massive postings have become a tool for manipulating social media debates. Here, it is significant to highlight that traditional media, especially television, have been suffering a constant process of wear and tear and discredit on the part of citizens. In this context, individuals to an increasing degree are using the Internet to acquaint themselves and trust in data obtained through the computer is superior to other media, such as newspapers, radio and television.[52] However, the *online* scenario is diffused by bots and algorithms that forge debate and change the priority of themes. In the course of the electoral race of 2018, automated accounts were responsible for 12.9% of interactions on Twitter.[53] In 2014, the first presidential election in which the robots had more meaningful performance, the interference was similar. The *bots* accounted for more than 10% of interactions on Twitter. Formerly during the Impeachment process of previous President Dilma Rousseff, the robots were answerable for 20% of the debate between supporters of Dilma. In the second round of the 2014 elections, 20% of the interactions in favour of Aécio Neves were brought forth by robots.[54]

---

consequences. (...) The use of the bots causes a polarization environment, since the internet has an increase in the flow of messages with the same content. In this scenario, says the researcher, it is difficult to come up with a spontaneous debate, with discordant and moderate ideas. 'This kind of action makes it difficult for more moderate positions to emerge. The search for a consensus is hampered because the robots can hijack part of the debate. " Cf. 'Research Shows that the Repercussion of the Cancellation of the Queermuseu was Inflated by Robots on the Internet' (*G1*, 2017) <https://g1.globo.com/rs/rio-grande-do-sul/noticia/pesquisa-demonstra-que-repercussao-do-cancelamento-do-queermuseu-foi-insuflada-por-robos-na-internet.ghtml> accessed 2 March 2017.

49 Ruediger (n 47).

50 'Robots, Social Networks and Politics in Brazil: Analysis of Interferences of Automated Profiles in the 2014 Elections' (*FGV DAPP*, 2018) <http://dapp.fgv.br/en/bots-social-networks-politics-brazil/> accessed 29 July 2019.

51 Ruediger (n 47).

52 Special Secretariat of Social Communication, Presidency of the Republic of Brazil, 'Brazilian Media Research 2016: Habits of Media Consumption by the Brazilian Population' (2016).

53'Robot-Influenced Debate Reaches 10.4% on Twitter' (*FGV DAPP*, 19 October 2018) <https://observa2018.com.br/posts/debate-influenciado-por-robos-volta-a-crescer-e-chega-a-104-das-discussoes-sobre-os-presidenciaveis-no-twitter/> accessed 29 October 2018.

54 Ruediger (n 47).

With this kind of maneuvering, robots produce the false sense of broad political support for a specific proposal, idea or public figure, alter the direction of public policies, interfere with the stock market, spread rumors, false news and conspiracy theories, produce inaccurate information and content, as well as entice users to hateful links that steal personal data, among other risks.[55] Note, nevertheless, that saying that these bots work in favor of a given agenda does not mean that they "entirely dominate the network, nor that the consequent perception of the larger part of the people will be the straight result of the influence of these devices".[56] What we ask to highlight are the dangers previously attained through the use of robots and the probable risks that are more and more close and reckless.

By interfering in developing debates in social networks, robots are directly reaching political and democratic processes through the influence of public opinion. Their actions may, for instance, create an artificial opinion, or unreal dimension of a certain opinion or public figure, by sharing versions of a particular theme, which expand in the network as if there were, among the part of society represented there, a very powerful opinion on a specific subject.[57]

The study of the use of robots already establishes clearly the adverse potential of this practice for the political dispute and the public debate.[58] One of the most apparent conclusions in this sense is the concentration of these actions in poles located at the extreme of the political spectrum, artificially promoting a radicalization of the debate in the bubble filters and, thereupon, undermining potential bridges of dialogue between the different political fields constituted. Therefore, the role of robots not only circulates false news, which can have damaging effects on society but also actively looks up to prevent users from informing

55On the existence today of an "army" of false profiles, cf. Juliana Gragnani, 'Exclusive: Investigation Reveals Army of Fake Profiles Used to Influence Elections in Brazil' *BBC News* (London, 8 December 2017) <https://www.bbc.com/portuguese/brasil-42172146> accessed 14 March 2018.

56 Ruediger (n 47) 8.

57 Yasodara Cordova and Danilo Doneda, 'A Place for the Robots (In the Elections)' (*JOTA*, 20 November 2017) <https://www.jota.info/opiniao-e-analise/artigos/um-lugar-para-os-robos-nas-eleicoes-20112017> accessed 9 March 2018.

58According to the research in Ruediger (n 47) 8 "The detection through machine learning occurs with the coding of behavior patterns from the collection of metadata. In this way, the system is able to automatically identify humans and robots based on the behavioral pattern of the profile. User metadata is considered one of the most predictable aspects of human and robot differentiation and can contribute to a better understanding of how sophisticated robots work. Identifying these robots or hacked accounts, however, is difficult for these systems. In addition, the constant evolution of robots causes the system, built from a static database, to become less accurate over time. However, it allows you to process a large number of complex correlations and patterns, as well as analyze a large number of accounts. The most efficient identification mechanisms combine different aspects of these approaches, exploring multiple dimensions of profile behavior, such as activity and time pattern. These systems take into account, for example, that real users spend more time on the network exchanging messages and visiting the content of other users, such as photos and videos, while robots accounts spend their time searching profiles and sending friendship requests."

themselves suitably.

Another familiar strategy of automated profiles is the sharing of spiteful links, which is targeted at the theft of personal data or information. This information - such as profile photos - can be used to produce new robotic profiles that have features that help them start connections on networks with real users. A common action, which generally generates distrust about the performance of robots, is the marking by an unrecognized user.

This kind of action indicates that social networks, used by so many people for information purposes, may certainly and paradoxically contribute to a less informed society by manipulating public debate. Taken together, these risks and others represented by the action of non-human artefacts (such as *bots*) are more than enough to shed light on a real threat to the quality of debate in the public sphere,[59] especially since nonhuman artefacts have been gaining momentum, autonomy and behavioural unpredictability.[60]

59 According to Habermas, *Law and Democracy* (n 8) 28-30, we must maximize the ideal speech conditions, that is, create an environment of democratic deliberation in which everyone has a voice. Faced with a scenario of crisis of representativity, the internet should be used as a tool for citizens to exercise their citizenship in an active way. According to Habermas, for democratic deliberation to occur, there are at least four conditions. These conditions, which characterize an "ideal speech situation", are basically linked to the need to guarantee the best conditions for deliberation and concern with the way the debate process is organized. They are: (i) each person must be able to express their own ideas openly and criticize those of others; (ii) the association of concepts of power and power with social status must be eliminated; (iii) arguments based on the appeal to tradition or dogma need to be exposed; and, as a consequence, the truth is achieved through the search for consensus.

60 In this sense, it is paradigmatic the example of the robot Tay, chatbot with capacity of deep learning created in 2016 by Microsoft. The experiment proved to be disastrous and the robot had to be deactivated within 24 hours of its start: Tay began to disseminate hate speech against historically marginalized minorities, stating for example that Hitler was right and that she hated Jews. About Robot Tay, cf. Isabela Moreira, 'Microsoft has Created a Robot that Interacts on Social Networks - and it has Become a Nazi' (*Galileo*, 24 March 2016) <https://revistagalileu.globo.com/blogs/buzz/noticia/2016/03/microsoft-criou-uma-robo-que-interage-nas-redes-sociais-e-ela-virou-nazista.html> accessed 29 October 2018.

5. FINAL CONSIDERATIONS

The latest developments in the new technologies addressed in this study alert us to the fact that the democratic role of the connected public sphere begins to run into risks and obstacles that can totally degrade its potential and should not be scrutinized enthusiastically as the panacea for salvation and legitimacy of the modern political system.

The hypertrophic impact of the market and bureaucratic economic rationality of the political system in the spheres of the world of life is seen by Habermas as one of the main pathologies of modernity, leading to loss of freedom and meaning in society.

Thus, the initial frenzy with the ideal of democratic virtual spheres and decolonization of the world of life provided by the new digital environments has lost its breath. Now that algorithms and other non-human agents are participating and influencing discourses in the public sphere, it is the question: will they be obligated to act morally and rationally-dialogically so that they do not negatively affect the ideal speech situation?

Many times there is a critical awareness of how the algorithms that make up the technologies work and how they can offer us personalized information from our personal data or even play upon our political vision. It is important to keep in mind that this operation often addresses political disputes or private business models that ask to maximize profit and not necessarily realize fundamental rights such as access to information, expression, and culture.

The Habermasian theory based on the logical and dialogical communicative concepts of the public sphere and ideal speech situation assists us to comply with how far we are distancing ourselves from a positive scenario from the perspective of democratic legitimacy. By the examination, we can conclude that the present situation is a colonization of the world of life established by non-human agents (bots, algorithms with artificial intelligence, among others) - and likewise by human agents, insofar as individuals also share and produce *fake news* and deep fakes-producing harmful consequences aggravated by the filter-bubble effects and the radicalization of discourses. Legal regulation must be attentive to these effects, seeking to correct them.

In the electoral context of 2018, fake news, in particular, and new technologies, in general, proved to be a challenging problem. On the one hand, controlling the broadcast and circulation of false news after its publication would be awfully dubious, given the rapid speed with which information is circulated in the context of the information society. On the other hand, prior

analysis of the truthfulness of the news stories could imply institutionalized forms of censorship.

It is mandatory, therefore, to formulize institutional forms of combat against fake news without one of the fears mentioned above materializing. Thus, indirect regulations are more likely to be effective in countering fake news, such as banning countless fake accounts and setting ethical standards for the use of algorithms and artificial intelligence.

Note, nevertheless, that legislating on these issues is extremely complicated, as we are dealing with essential principles of democracy, such as freedom of expression and right of access to information. But this still seems to be the most appropriate alternative in the short and medium-term. There are technologies that can be used in smartphones and computers to realize the truthfulness of some information.[61] However, it is a technology of high value, which demands infrastructure and the replacement of devices that already circulate today. That is, it is a long-term measure and with many difficulties to be faced, such as those related to the privacy of technology users.

As we can observe, every day the new technologies are applying a greater influence on the life of the citizens and in the way they look at the facts. This impact expands more and more into all areas of our lives and has recently hit the elections thoroughly. Although it is not yet possible to say that algorithmic manipulation, bot use, fake news and deep fake disclosure are largely responsible for the election results, we can say that we are moving towards a scenario where it would be possible to hack the electoral process.

61 Viana and Zanatta (n 3).

6. REFERENCES

Adam Liptak, 'Sent to Prison by a Software Program's Secret Algorithms' The New York Times (1 May 2017) <https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html?mtrref=www.google.com.br&gwh=B3F9140AAAB1DACDFCE11CBD55F4DB8F&gwt=pay> accessed 29 October 2017.

Aviv Ovadya, 'What's Worse Than Fake News? The Distortion Of Reality Itself' [2018] 35(2) New Perspectives Quarterly 43-45.

Benjamin Lee, 'Marina Abramović Mention in Podesta Emails Sparks Accusations of Satanism' The Guardian (4 November 2016) <https://www.theguardian.com/artanddesign/2016/nov/04/marina-abramovic-podesta-clinton-emails-satanism-accusations> accessed 29 October 2018.

Brazilian Media Survey 2016 (Pesquisa de Media, 2016) <https://bit.ly/2YH6udr> accessed 29 October 2016.

Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach' The Guardian (17 March 2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> accessed 29 April 2017.

Cass Sunstein, Republic.com (Princeton University Press 2001).

Cass Sunstein, Republic.com 2.0 (Princeton University Press 2009)

Clara Velasco and Roney Sundays, 'What is a Web Robot and How Can it Influence the Debate in Networks? Experts Explain' (G1, 2017) <https://g1.globo.com/economia/tecnologia/noticia/o-que-e-um-robo-na-web-e-como-ele-pode-influenciar-o-debate-nas-redes-especialistas-explicam.ghtml> accessed 29 October 2017.

Coalition of Rights on the Network, 'Fake News and Elections' (Rights on the Net, 2017) <https://direitosnarede.org.br/p/carta-aberta-americalatinaecaribe-igf2017/> accessed 29 October 2017.

Craig Silverman, 'Here Are 50 of the Biggest Fake News Hits on Facebook From 2016'

(BuzzFeed News, 30 December 2016) <https://www.buzzfeednews.com/article/craigsilverman/top-fake-news-of-2016#.nl712lkw2> accessed 29 October 2018

Eduardo Gianetti, Lies We Live By: The Art of Self-deception (Companhia das Letras 2005)

Eduardo Magrani and others, Terms of Service and Human Rights: An Analysis of Online Platform Contracts (Revan 2016).

Eduardo Magrani and Renan Medeiros de Oliveira, 'We are Big Data: New technologies and Personal Data Management' (2018) 5 CyberLaw 10-33 <http://www.cijic.org/publicacao/> accessed 29 July, 2019.

Eduardo Magrani, 'The Internet of Things: Privacy and Ethics in the Age of Hyperconnectivity' (Pontifical Catholic University of Rio de Janeiro 2018).

Eduardo Magrani, Connected Democracy: The Internet as a Tool for Political-Democratic Engagement (Juruá 2014).

Eduardo Magrani, The Internet of Things (FGV Editora 2018).

Eli Pariser, The Filter Bubble: What the Internet is Hiding from You (Penguin Press 2011).

Evgeny Morozov, To Save Everything, Click Here: The Folly of Technological Solutionism (Public Affairs 2013)

Frank Pasquale in Frank Pasquale, The Black Box Society: The Secret Algorithms that Control Money and Information (Harvard University Press 2015).

Gabriela Fujita, 'SP: Datafolha shows France with 51% and Doria, 49%; Ibope brings 50% for each' UOL (Sao Paulo, 27 October 2018) <https://noticias.uol.com.br/politica/eleicoes/2018/noticias/2018/10/27/datafolha-ibope-sp-doria-franca.htm> accessed 29 October 2018.

Institute of Technology and Equity, 'Experts Explain How the Robot can Influence the Debate in Networks' (Medium, 15 December 2017) <https://medium.com/@tecnoequidade/especialistas-explicam-como-o-robô-pode-influenciar-o-debate-nas-redes-3a844f911849> accessed 29 October 2017.

Isabela Moreira, 'Microsoft has Created a Robot that Interacts on Social Networks - and it has Become a Nazi' (Galileo, 24 March 2016) <https://revistagalileu.globo.com/blogs/buzz/noticia/2016/03/microsoft-criou-uma-robo-que-

interage-nas-redes-sociais-e-ela-virou-nazista.html> accessed 29 October 2018.

James Bohman and William Rehg., 'Jürgen Habermas' The Stanford Encyclopedia of Philosophy (2007) <https://plato.stanford.edu/entries/habermas/> accessed 29 July 2019.

Joshua Cohen, 'Deliberation and Democratic Legitimacy' in James Bohman and William Rehg (eds), Deliberative Democracy: Essays on Reason and Politics (MIT Press 1997) 29.

Julia Lane and others (eds), Privacy, Big Data and the Public Good: Frameworks for Engagement (CUP 2014).

Juliana Gragnani, 'Exclusive: Investigation Reveals Army of Fake Profiles Used to Influence Elections in Brazil' BBC News (London, 8 December 2017) <https://www.bbc.com/portuguese/brasil-42172146> accessed 14 March 2018.

Jürgen Habermas, Strukturwandel der Öffentlichkeit (Structural Transformation of the Public Sphere) (English edn, Polity 1989).

Jürgen Habermas. Law and Democracy: Between Facticity and Validity, vol 2 (2nd edn, Tempo Brasileiro 2003) 16.

Jürgen Habermas. The Theory of Communicative Action, vol 2 (Beacon Press 1987) 113-197; Craig Calhoun (ed), Habermas and the Public Sphere (MIT Press 1992) 1-51.

Marco Aurélio Ruediger, 'Robots, Social Networks and Politics in Brazil: Study on Illegitimate Interference in the Public Debate on the Web, Risks to Democracy and the Electoral Process of 2018' (FGV DAPP, 2018) <http://dapp.fgv.br/en/robots-social-networks-politics-fgv-dapp-study-points-illegitimate-interference-public-debate-web/> accessed 29 July 2019 (Ruediger).

Mariana Simões, 'Pro-Bolsonaro Groups on WhatsApp Orchestrate Fake news and Personal Attacks on the Internet, Research Says' El País (24 October 2018) <https://brasil.elpais.com/brasil/2018/10/23/politica/1540304695_112075.html?id_externo_rsoc=FB_BR_CM&fbclid=IwAR05Mw9zXzmjDbYv5OkjAm1hVipWBURMCPyiOORIaxSsy_qNxEjzrpHKxfQ> accessed 29 October 2018.

Natalia Viana and Carolina Zanatta, 'Deep Fakes are Threatening on the Horizon, But They Are Not Yet a Weapon for Elections, Says Expert' The Public (16 October 2018) <https://apublica.org/2018/10/deep-fakes-sao-ameaca-no-horizonte-mas-ainda-nao-sao-arma-para-eleicoes-diz-especialista> accessed 25 October 2018.

Patricia Campos Mello, 'Entrepreneurs Campaign Against the PT by WhatsApp' (Folha de São

Paulo, 18 October 2018) <https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml> acessed 29 October 2018.

Pedro Ortellado, 'Bias on the Internet Does Not Seem to Be Caused by "Bubbles"' (Folha de São Paulo, 2018) <https://www1.folha.uol.com.br/colunas/pablo-ortellado/2018/02/polarizacao-na-internet-nao-parece-ser-causada-pelas-bolhas.shtml> accessed 29 October 2018.

Redação Pragmatismo, 'Intimate video of João Doria is true, new report points out' (Pragmatismo Político, 26 October 2018) <https://www.pragmatismopolitico.com.br/2018/10/video-intimo-joao-doria-verdadeiro-pericia.html> accessed 29 October 2018.

Rolf Wiggershaus and others, The Frankfurt School: Its History, Theories, and Political Significance (MIT Press 1995).

Sérgio Quintella, 'Expertise Reveals Report on Intimate Video Attributed to João Doria' Veja São Paulo (24 October 2018) <https://vejasp.abril.com.br/blog/poder-sp/pericia-aponta-montagem-em-video-intimo-atribuido-a-joao-doria/> accessed 29 October 2018.

Special Secretariat of Social Communication, Presidency of the Republic of Brazil, 'Brazilian Media Research 2016: Habits of Media Consumption by the Brazilian Population' (2016).

Tim Wu. The Master Switch: The Rise and Fall of Information Empire (Vintage 2011).

Yasodara Cordova and Danilo Doneda, 'A Place for the Robots (In the Elections)' (JOTA, 20 November 2017) <https://www.jota.info/opiniao-e-analise/artigos/um-lugar-para-os-robos-nas-eleicoes-20112017> accessed 9 March 2018.

'"Voter Fraud" and "Gay Kit" Have a Greater Impact than Other Fake Twitter, Facebook and Youtube News' (FGV DAPP, 1 Novemeber 2018) <https://observa2018.com.br/posts/fraude-nas-urnas-e-kit-gay-tem-maior-impacto-que-outras-noticias-falsas-em-twitter-facebook-e-youtube/> accessed 29 October 2018.

'How Russia-Linked Hackers Stole the Democrats' Emails and Destabilized Hillary Clinton's Campaign' ABC News (5 November 2017) <https://www.abc.net.au/news/2017-11-04/how-russians-hacked-democrats-and-clinton-campaign-emails/9118834> accessed 29 October 2018.

'Privacidade No Facebook: o que aprender com a Cambridge Analytica' (Irisbh, 19 March 2018) <http://irisbh.com.br/privacidade-no-facebook-cambridge-analytica/> accessed 28

October 2018.

‘Research Shows that the Repercussion of the Cancellation of the Queermuseu was Inflated by Robots on the Internet’ (G1, 2017) <https://g1.globo.com/rs/rio-grande-do-sul/noticia/pesquisa-demonstra-que-repercussao-do-cancelamento-do-queermuseu-foi-insuflada-por-robos-na-internet.ghtml> accessed 2 March 2017.

‘Robot-Influenced Debate Reaches 10.4% on Twitter’ (FGV DAPP, 19 October 2018) <https://observa2018.com.br/posts/debate-influenciado-por-robos-volta-a-crescer-e-chega-a-104-das-discussoes-sobre-os-presidenciaveis-no-twitter/> accessed 29 October 2018.

‘Robots, Social Networks and Politics in Brazil: Analysis of Interferences of Automated Profiles in the 2014 Elections’ (FGV DAPP, 2018) <http://dapp.fgv.br/en/bots-social-networks-politics-brazil/> accessed 29 July 2019.

‘There are 7 Types of Fake News. Do You Know Them All?’ (Magic Web Design, 19 March 2018) <https://www.magicwebdesign.com.br/blog/internet/existem-7-tipos-fake-news-voce-conhece-todos/> accessed 29 October 2018.

CYBERLAW
by CIJIC

A INVESTIGAÇÃO DO CIBERCRIME - NÓTULAS SOBRE O PARADIGMA LEGISLATIVO ATUAL E A REALIDADE TECNOLÓGICA

ARMANDO DIAS RAMOS [1]

1 Doutor em Direito – Ciências Jurídicas, pela Universidade Autónoma de Lisboa; Inspetor chefe na Polícia Judiciária, colocado na Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T); Professor Adjunto convidado no ISCAL-IPL; Editor assistente na Revista Brasileira de Direito Processual Penal. O presente artigo vincula apenas o seu autor e de nenhum modo as instituições anteriormente mencionadas.

ABSTRACT

In the 10th anniversary of the Portuguese cybercrime law we focused on legislative and technological developments in order to ascertain whether the legal norms we have are sufficient for effective criminal combat.

Among the many issues we identified, we look at the issue of using email and the undercover agent.

Indeed, the lack of modern instruments already used by several foreign counterparts in cybercrime investigation leads us to the conclusion that we need harmonized and more concrete legal instrument for a fast, fruitful and efficient investigation.

There is a need to change the current paradigm by imposing a change in the Portuguese cybercrime law.

Keywords: Portuguese Cybercrime law; Criminal investigation; judicial cooperation; cybercrime; e-mail; undercover agent.

RESUMO

Nos 10 anos da lei do cibercrime debruçamo-nos sobre a evolução legislativa e tecnológica com o intuito de apurar se as normas legais que temos são suficientes para um efetivo combate ao crime.

De entre diversos problemas que identificamos, analisamos a questão relacionada com a utilização do correio eletrónico e o agente encoberto.

Efetivamente a falta de instrumentos modernos, já utilizados por diversas congéneres estrangeiras na investigação de cibercrimes conduzem-nos à conclusão de que necessitamos de leis harmonizadoras e mais concretas, para uma investigação célere, profícua e eficiente.

Urge mudar o atual paradigma e impõe-se uma alteração da lei do cibercrime.

Palavras-chave: Lei do Cibercrime; Investigação criminal; cooperação judiciária; cibercriminalidade; correio eletrónico; agente encoberto.

1. INTRODUÇÃO

A 15 de setembro de 2019 faz 10 anos que a atual lei do cibercrime, Lei 109/2009, foi publicada. Passado um mês, a 15 de outubro de 2009, entrou em vigor e veio revogar, desta forma, a anterior lei da criminalidade informática[1].

Se, efetivamente, a lei da criminalidade informática esteve em vigor 18 anos, sofrendo apenas uma ligeira alteração, pelo decreto-lei n.º 323/2001, de 17 de dezembro, por força da introdução do euro como moeda em curso no nosso país, a atual lei, 10 anos depois, não sofreu qualquer alteração legislativa[2]. Contudo, se atentarmos à evolução da informática nos idos anos 90, do século passado, com os últimos 10 anos constatamos, indubitavelmente, que se passou de uma evolução de "passo de tartaruga" para "uma corrida de lebre", na breve alusão à fábula da corrida entre a tartaruga e a lebre.

Eis, pois, que se impõe refletir sobre estes 10 anos da lei do cibercrime, da evolução tecnológica operada nesta década e, principalmente, da evolução da cibercriminalidade e meios efetivos de combate. Não podemos olvidar os problemas associados à investigação do cibercrime, muitos deles já identificados, onde se destacam a desterritorialidade e a anonimização como matrizes para propalar a atividade delituosa.

Estará a lei do cibercrime devidamente atual face aos novos e cada vez mais complexos artefactos utilizados no cometimento de delitos informáticos ou por via informática? Deverá a investigação criminal, para ser mais célere, recorrer a vias informais, tanto a nível nacional como com as congéneres estrangeiras, para lograr o êxito de identificação dos criminosos e os entregar à Justiça?

Estas são algumas perguntas (problemas) que levantamos e que tentaremos dar resposta. Desde já fica o alerta que as instâncias europeias se têm preocupado com estes fenómenos criminológicos e definindo uma "agenda digital" para o combate à cibercriminalidade. Contudo, face à globalização da internet, bastarão as medidas europeias para um eficaz combate? Não restam dúvidas que atenuam os efeitos do cibercrime e ajudam a minimizar o problema. Ainda assim não poderemos olvidar que grandes empresas, presentes na Europa, são norte americanas, onde se destacam a Google e o Facebook, ou chinesas, tais como a Amazon e a Alibaba.

Os problemas agudizam-se fora da Europa uma vez que se torna mais difícil obter elementos conducentes à identificação dos suspeitos ou à recolha de prova digital. Efetivamente os mecanismos adotados, por diversas empresas estrangeiras, já permitem uma

1 Lei n.º 109/91, de 17 de agosto.
2 Encontrando-se Portugal em incumprimento uma vez que já deveria ter adaptado para o direito interno a Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013.

celeridade na obtenção de elementos de provas. Desde logo deixou de ser necessário a emissão de cartas rogatórias bastando que o pedido seja efetuado por *e-mail*, emanado da autoridade judiciária competente, certificado pela respetiva assinatura digital. Também foram criados mecanismos protocolares entre essas empresas e as autoridades judiciárias portuguesas, no sentido de acelerarem os pedidos de informações e obtenção de elementos que, a ser obtidos por carta rogatória, poderiam tornar-se demasiado demorados.

A investigação do cibercrime não assenta somente em elementos técnicos e informáticos, mas estes são o cerne da questão por diversos fatores. Enquanto que num crime de cenário é possível a recolha de elementos que nos levam quase indubitavelmente ao que ali sucedeu e, eventualmente, de quem foram os seus agentes – veja-se a título de exemplo um crime de homicídio ou de roubo. Nos crimes informáticos é, na maioria das vezes, difícil percecionarmos quais as provas que necessitamos recolher em função do tipo de crime em investigação. O avanço tecnológico traz consigo a mudança de paradigma de *modus operandi*, apanhando desprevenidos não só os investigadores, mas essencialmente as vítimas.

Acompanhamos as palavras de JOSÉ BRAZ quando nos diz que "*a investigação criminal se desenvolve, basicamente, em duas estratégias (...) num quadro de permanente interatividade e integração (...) – o conjunto de procedimentos tendentes à obtenção da prova pessoal (interrogação) e, - o conjunto de procedimentos tendentes à obtenção da prova material (instrumentação)*"[3].

Se a investigação criminal na área do cibercrime necessita de evoluir, por força das novas tecnologias, a lei terá que acompanhar este progresso, dando mais ferramentas aos investigadores e aos julgadores para que a justiça seja feita.

3 JOSÉ BRAZ, *Investigação Criminal, a organização, o método e a prova, Os desafios da nova criminalidade*, Almedina, 2009, p. 20.

2. A ATUAL LEI DO CIBERCRIME

A atual lei do cibercrime teve a sua génese na transposição para a ordem jurídica interna da Decisão Quadro n.º 2005/222/JAI[4], do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa[5]. Nesta Decisão Quadro ficou estabelecido que os Estados-Membros deveriam tomar as medidas necessárias para dar cumprimento às suas disposições até 16 de Março de 2007. Ora, volvidos mais de dois anos a Decisão Quadro foi finalmente transposta para o nosso ordenamento jurídico. Por outro lado, com a ratificação da Convenção de Budapeste, criaram-se novos tipos legais de crime, usando a terminologia ali adotada.

A lei do cibercrime comporta diversos tipos legais de crime. Nela se encontram os crimes de falsidade informática (art. 3.º), dano relativo a programas ou outros dados informáticos (art. 4.º), sabotagem informática (art. 5.º), acesso ilegítimo (art. 6.º), interceção ilegítima (art. 7.º) e reprodução ilegítima de programa protegido (art. 8.º).

A inovação da lei do cibercrime verifica-se, para além dos tipos legais de crime, pela possibilidade da admissão de recolha de elementos de prova que não se encontravam previstos no código de processo penal. Admissibilidade esta que vai mais além da existente e se aplica, nos termos do art. 11.º, a todos os tipos de crime, não só a esta lei, mas a todos os ilícitos penais que sejam cometidos por via informática ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico.

Criou-se, deste modo, a possibilidade de efetuar a preservação e a revelação expedita de dados (art. 12.º e 13.º, respetivamente), injunção para apresentação ou concessão do acesso a dados (14.º), pesquisa e apreensão de dados informáticos (art. 15.º e 16.º, respetivamente), apreensão de correio eletrónico e registo de comunicações de natureza semelhante (art. 17.º), interceção de comunicações (art. 18.º) e ações encobertas (art. 19.º).

Destarte, também saiu reforçada a cooperação internacional com o principal mecanismo previsto na Convenção de Budapeste, isto é, a criação de um ponto de contacto permanente[6]. Este *focal point* tem em vista a assistência imediata para que as autoridades nacionais competentes cooperem com as autoridades estrangeiras competentes para efeitos de investigações ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos, bem como para efeitos de recolha de prova, em suporte eletrónico.

---

4 Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32005F0222 [acedido em 23 de junho de 2019]. Esta Decisão Quadro foi substituída pela Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação.

5 Também designada por Convenção de Budapeste, por ter sido assinada naquela cidade em 23 de novembro de 2001.

6 Também conhecido por 24/7. Este ponto de contacto ficou sob a égide da Polícia Judiciária, por ser o Órgão de Polícia Criminal com competência, nos termos da LOIC, para a investigação dos crimes informáticos.

Se atentarmos nas normas europeias verificamos que a diretiva que deu origem à nossa lei do cibercrime foi substituída pela Diretiva 2013/40/UE, do Parlamento Europeu e do Conselho, foi publicada no Jornal Oficial da União Europeia em 12 de agosto de 2013.

O imperativo de transposição, para o ordenamento jurídico interno, surge na Diretiva 2013/40/UE que expressamente refere no seu art. 16.º, n.º 1, que "*os Estados-Membros põem em vigor as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à presente diretiva até 4 de setembro de 2015*." Efetivamente, como já mencionamos anteriormente, há muito que foi ultrapassado o prazo para a transposição, não se compreendendo este lapso temporal para tal. Como é referido no Relatório do Ministério dos Negócios Estrangeiros – "Portugal na União Europeia Ano 2013" "*[Q]uanto à diretiva relativa aos ataques contra os sistemas de informação, a sua transposição também não deverá exigir grande esforço legislativo, atendendo à disciplina já contida na Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime)*[7]."

Esta Diretiva tem como objeto aproximar as infrações penais no domínio de ataques contra sistemas de informação dos Estados-Membros e estabelecer regras mínimas relativas às sanções aplicáveis e respetivas infrações. Visa também, segundo o seu art. 1.º, a introdução de disposições comuns para prevenir tais ataques e melhorar a cooperação entre as autoridades judiciais e outras autoridades competentes europeias neste domínio[8].

Centrando-nos na atual lei do cibercrime, verificou-se que a sua interpretação, quando entrou em vigor e durante os primeiros anos, não foi fácil de efetuar. Desde logo a confusão operada por dados de base, dados de tráfego, dados de conteúdo, etc. Que autoridade judiciária poderia efetuar, por exemplo, junto das operadoras de comunicações determinado pedido? O Ministério Público ou obrigatoriamente o Juiz de Instrução Criminal? Tal celeuma deu origem a acórdãos dos tribunais superiores em sentido diverso, bem como a interpretações doutrinais diferentes[9].

Outros problemas surgiram por via da interpretação doutrinária. O art. 11.º, n.º 2 refere que "as disposições processuais previstas no presente capítulo não prejudicam o regime da Lei n.º 32/2008, de 17 de julho". Gerou-se a dúvida se a Lei de Retenção de dados se aplicava a todos os tipos legais existentes na Lei do Cibercrime ou apenas aos crimes graves[10].

---

7 Disponível em http://app.parlamento.pt [acedido em 12 de julho de 2019]. Relatório não datado mas pela sua leitura e análise que faz do ano de 2013 é de prever que tenha sido elaborado no decurso de 2014.

8 Para um estudo mais aprofundado sobre esta Diretiva, remetemos para o nosso artigo "A novíssima Diretiva relativa ao cibercrime", In SOUSA, CONSTANÇA URBANO DE (Coord.), *O Espaço de liberdade, segurança e justiça da UE: desenvolvimentos recentes*, EDIUAL, Lisboa, maio de 2014, pp. 176 a 192.

9 DUARTE RODRIGUES NUNES, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, Gestlegal, 2018, pp. 32 e ss; PEDRO VERDELHO, "Cibercrime", in *Dicionário da Sociedade de Informação*, IV, p. 376, e também em "A Convenção sobre o Cibercrime do Conselho da Europa – Repercussões na Lei Portuguesa", in *Direito da Sociedade da Informação*, VI, pp. 270-271; DAVID SILVA RAMALHO, "A investigação criminal na Dark Web", in *Revista da Concorrência e Regulação*, n.º 14/15, pp. 398-399.

10 Definindo esta lei, art. 2.º, n.º 1, alínea g), que por crime grave se entende os crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a

Efetivamente esta amálgama de legislação confusa, deixando ao intérprete uma ampla margem de defesa das suas posições aquando da interpretação da norma jurídica, leva o a que a certeza do Direito, *maximus*, princípio da certeza jurídica, ínsito no art. 2.º da Constituição da República, deixe de o ser tão certo. Contudo, temos constatado a falta de invocação, em sede própria, da validade da Lei n.º 32/2008[11]. É certo que se trata de uma lei gerada no seio da Assembleia da República e que cumpre todos os requisitos de aplicabilidade interna, mas tratando-se da transposição de uma Diretiva europeia, como mencionamos supra, que recentemente foi considerada inválida pelo Tribunal de Justiça da União Europeia, manterá esta validade sem mácula[12]? Poderá existir algum recurso que afaste a sua aplicabilidade legal?

Acresce, sendo de extrema importância, que a salvaguarda de dados de tráfego é condição *si ne quo non* para a identificação dos presumíveis autores de qualquer ilícito informático ou praticado através de meios informáticos. Manter-se-á válida a definição legislativa de "dados de tráfego" inserida na Lei do cibercrime ou estará a mesma desadequada face à realidade tecnológica?

Analisaremos de seguida o acórdão do TJUE uma vez que sem dados informáticos a investigação criminal, a nível do cibercrime, não poderá atingir os seus objetivos e consequentemente lograr-se uma profícua investigação, ou seja, a identificação dos autores da prática dos crimes.

identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou títulos equiparados a moeda e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima.

11 A Provedora de Justiça, em 29/01/2019, endereçou uma recomendação à Ministra da Justiça no sentido de alterar a Lei n.º 32/2008, de 17 de julho, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações. Vide https://www.provedor-jus.pt/?idc=35&idi=17775 [*acedido em 27 de agosto de 2019*]. Mais recentemente, a 27 de agosto de 2019 a Provedora de Justiça solicitou ao Tribunal Constitucional a fiscalização abstrata da constitucionalidade dos art.s 4.º, 6.º e 9.º, da Lei n.º 32/2008.

12 No sentido do que acabamos de referir veja-se Ac. TRL, Proc. 8617/17.8T9LSB-A.L1-3, de 28-11-2018, Relator: Conceição Gonçalves, in www.dgsi.pt [acedido a 26 de agosto de 2019].

3. ANÁLISE DO ACÓRDÃO DO TRIBUNAL DE JUSTIÇA, DE 8 DE ABRIL DE 2014.

O Tribunal de Justiça da União Europeia (TJUE) foi chamado a pronunciar-se, em 12 de junho de 2012, em virtude do *High Court of Ireland* ter suscitado uma questão prejudicial sobre a validade da Diretiva 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, em face dos Tratados (Processo C-293/12). Da mesma forma, em 19 de dezembro de 2012 e com uma argumentação algo distinta, o *Verfassungsgerichtshof* (Áustria) suscitou também, junto do TJUE, uma questão prejudicial sobre a validade da Diretiva 2006/24/CE em face dos Tratados (Processo C-594/12). Este processo por ser semelhante ao pedido da Irlanda ficou apenso ao mesmo.

O pedido apresentado pela High Court é relativo a um litígio que opõe a Digital Rights Ireland Ltd. (a seguir «Digital Rights») ao Minister for Communications, Marine and Natural Resources, ao Minister for Justice, Equality and Law Reform, ao Commissioner of the Garda Síochána, à Irlanda e ao Attorney General acerca da legalidade de medidas legislativas e administrativas nacionais respeitantes à conservação de dados relativos a comunicações eletrónicas. Ou seja, tratava-se de determinar se uma vigilância em massa é compatível com a salvaguarda dos Direitos Fundamentais, tal como constam da Carta e da Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais.

Concretamente:

1) A Diretiva 2006/24/CE é compatível com o direito dos cidadãos de circularem e permanecerem livremente no território dos Estados-Membros, consagrado no artigo 21.° TFUE?;

2) A Diretiva 2006/24/CE é compatível com o direito ao respeito pela vida privada, consagrado no artigo 7.° da Carta [dos Direitos Fundamentais da União Europeia (a seguir 'Carta')] e no artigo 8.° da [CEDH]? [13];

13 CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA (2010/C 83/02), publicada no Jornal Oficial da União Europeia, em 30/03/2010, estabelecendo:
Artigo 7.º-Respeito pela vida privada e familiar:
Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.
Artigo 8.º - Proteção de dados pessoais:
1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação.
3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.
Artigo 11.º -Liberdade de expressão e de informação:
1. Qualquer pessoa tem direito à liberdade de expressão. Este direito compreende a liberdade de opinião e a liberdade de receber e de transmitir informações ou ideias, sem que possa haver ingerência de quaisquer poderes públicos e sem consideração de fronteiras.
2. São respeitados a liberdade e o pluralismo dos meios de comunicação social.

3) A Diretiva 2006/24/CE é compatível com o direito à proteção dos dados pessoais, consagrado no artigo 8.° da Carta?;

4) A Diretiva 2006/24/CE é compatível com o direito à liberdade de expressão, consagrado no artigo 11.° da Carta e no artigo 10.° da CEDH?;

5) A Diretiva 2006/24/CE é compatível com o direito a uma boa administração, consagrado no artigo 41.° da Carta?;

6) Em que medida os Tratados e, em concreto, o princípio da cooperação leal previsto no artigo 4.°, n.° 3, TUE, exigem que os tribunais investiguem e apreciem a compatibilidade das medidas nacionais de transposição da Diretiva 2006/24/CE com as garantias conferidas pela Carta, incluindo o seu artigo 7.° (cujo conteúdo é inspirado no artigo 8.° da CEDH)?

O pedido apresentado pelo *Verfassungsgerichtshof* é relativo a recursos em matéria constitucional interpostos perante este órgão jurisdicional respetivamente pelo Kärntner Landesregierung (Governo do Land de Caríntia), bem como por M. Seitlinger, C. Tschohl e 11 128 outros recorrentes, acerca da compatibilidade da lei que transpõe a Diretiva 2006/24 para o direito interno austríaco com a lei constitucional federal (*Bundes-Verfassungsgesetz*). Essencialmente, trata-se de determinar se os art.ºs 3.º a 9.º da Diretiva são compatíveis com os art.ºs 7.º, 8.º e 11.º[14] da Carta dos Direitos Fundamentais da EU, assim como, qual a relevância, *in casu*, *"[…] do Princípio da salvaguarda de um nível de proteção mais elevado, consagrado no artigo 53.º da Carta?"*; e, ainda, se *"[…] é possível deduzir da jurisprudência do Tribunal Europeu dos Direitos Humanos em relação ao artigo 8.º da CEDH a existência de elementos de interpretação do artigo 8.º da Carta que possam influenciar a interpretação deste último artigo?"*

Numa sociedade cada vez mais informatizada coloca-se em causa a proteção de dados pessoais, a liberdade de cada indivíduo e o respeito pela sua privacidade.

A decisão tomada pela Grande Secção do TJUE vem debruçar-se sobre este assunto e em particular à Diretiva 2006/24, que deu origem à nossa Lei n.º 32/2008. Neste aspeto referem os doutos magistrados daquela instância europeia que "*limitando-se a dispor que cada Estado-Membro define os procedimentos que devem ser seguidos e as condições que devem ser respeitadas para se ter acesso a dados conservados de acordo com os requisitos da necessidade e da proporcionalidade. Em particular, a Diretiva 2006/24 não estabelece um critério objetivo que permita limitar o número de pessoas com autorização de acesso e de utilização posterior dos dados conservados ao estritamente necessário à luz do objetivo prosseguido. O acesso aos dados conservados pelas autoridades nacionais competentes não está sobretudo sujeito a um controlo prévio efetuado por um órgão jurisdicional ou por uma entidade administrativa independente cuja decisão vise limitar o acesso aos dados e a utilização dos mesmos ao estritamente necessário para alcançar o objetivo prosseguido e*

14 A UE não só está vinculada pela sua Carta dos Direitos Fundamentais, mas também pela CEDH e pelas tradições constitucionais comuns aos Estados membros (Art.º 6.º do TUE).

ocorra na sequência de um pedido fundamentado destas autoridades apresentado no âmbito de procedimentos de prevenção, deteção ou ação penal. Também não foi prevista uma obrigação precisa de os Estados-Membros estabelecerem tais limitações."

Destarte tal não configurar uma obrigação dos Estados-Membros previsto na Diretiva, certo é que em Portugal o art. 8.º da Lei n.º 32/2008 estipula que a Comissão Nacional de Proteção de Dados (CNPD) deve manter um registo eletrónico permanentemente atualizado das pessoas especialmente autorizadas a aceder aos dados, nos termos da alínea d) do n.º 1 do artigo anterior. Desconhece-se até que ponto tal obrigação, por parte dos operadores nacionais, está a ser cumprida e devidamente fiscalizada pela CNPD. A este respeito recordamos que o art. 10.º da Lei n.º 32/2008 estabelece que a transmissão dos dados referentes às categorias previstas no artigo 4.º processa-se mediante comunicação eletrónica, nos termos das condições técnicas e de segurança previstas no n.º 3 do artigo 7.º. Esta transmissão veio posteriormente a ser regulamentada através da Portaria n.º 469/2009, de 6 de maio[15], que estabelece as regras sobre a transmissão de dados de forma eletrónica entre magistrados e os ISP's. Na prática tal sistema não se encontra em funcionamento[16] e levou inclusive a que a Procuradoria Geral da República firmasse um acordo com as operadoras que prestam serviços de Internet (ISP)[17]. Pelo que será de duvidar da eficácia deste artigo e nesse sentido damos razão aos magistrados do TJUE quando afirmam neste acórdão que "*a Diretiva 2006/24 não estabelece regras claras e precisas que regulem o alcance da ingerência nos direitos fundamentais consagrados nos artigos 7.° e 8.° da Carta. Impõe-se pois concluir que esta diretiva comporta uma ingerência*

15 Estabelece os termos das condições técnicas e de segurança em que se processa a comunicação eletrónica para efeitos da transmissão de dados de tráfego e de localização relativos a pessoas singulares e a pessoas colectivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, nos termos previstos na Lei n.º 32/2008, de 17 de julho.

16 Esta Portaria estabelece, no n.º 1, do Art. 2.º, que o juiz que tenha ordenado ou autorizado a transmissão de dados nos termos previstos no artigo 9.º da Lei n.º 32/2008, de 17 de Julho, comunica a decisão através da aplicação informática denominada 'sistema de acesso ou pedido de dados às operadoras de comunicações' (SAPDOC) especificamente disponibilizada para o efeito (*negrito nosso*).

17 Este protocolo foi assinado em 9 de julho de 2012 e estabeleceu um formulário tipo para o pedido de identificação de um titular de um IP, encontra-se acessível no *site* da PGR em http://www.pgr.pt/Protocolos/PROTOCOLO-comunicacoes.pdf. Posteriormente a PGR, através da Circular 12/2012, de 25/09/2012 esclarece os magistrados do Ministério Público que foi criado no SIMP (Sistema de Informação do Ministério Público) uma plataforma eletrónica para solicitar os pedidos às operadoras. Acrescenta-se, por isso, que enquanto não se mostrar possível a utilização da nova plataforma eletrónica do SIMP, os formulários serão impressos em papel e remetidos pelas vias habituais. Procedimento este que ainda hoje em dia é utilizado pelo Ministério Público para solicitar dados às operadoras de comunicações. Referida circular encontra-se disponível ao público no *site* da PGR, no endereço http://www.pgr.pt/Circulares/textos/2012/circular_12-2012.pdf [*acessos efetuados em 20 de agosto de 2019*].
Uma nótula relativa a este Protocolo que, em nossa modesta opinião, inverte os papéis da Justiça em Portugal, ao permitir que sejam os operadores, que acabam por ter acesso a informações que não necessitam, a decidir que dados fornecem ou não às autoridades judiciárias. O Ministério Público ou o JIC não deveriam informar os ISP's ao abrigo de que legislação requerem os dados de identificação de determinado cliente, num grupo data/hora e fuso horário. As interpretações da lei são da competência dos Tribunais e não de juristas de empresas de comunicações, cabendo aos Tribunais a aplicação da Lei, no estrito dever de legalidade, necessidade e proporcionalidade. Caso dúvidas subsistam, seja pela defesa, seja pelo MP, existem, para o efeito, os Tribunais de recurso. Discordamos totalmente da forma como foi construído este formulário bem como o objetivo final do protocolo: a cedência de informação por parte dos operadores que a Lei determina que seja fornecida obrigatoriamente no âmbito de um inquérito crime, cominando a desobediência com obstrução á justiça e a não salvaguarda de dados de tráfego com a aplicação de uma contraordenação.

nestes direitos fundamentais de grande amplitude e particular gravidade na ordem jurídica da União, sem que essa ingerência seja enquadrada com precisão por disposições que permitam garantir que a mesma se limita efetivamente ao estritamente necessário" e "*a Diretiva 2006/24 não estabelece regras específicas e adaptadas à grande quantidade de dados cuja conservação é imposta por esta diretiva, ao caráter sensível destes dados e ao risco de acesso ilícito aos mesmos, regras que se destinariam designadamente a regular de maneira clara e estrita a proteção e a segurança dos dados em causa, a fim de garantir a sua plena integridade e confidencialidade.*"

Mas o cerne da questão aflorado no arresto em análise refere-se que a Diretiva não impõe, quanto aos dados salvaguardados, que os mesmos sejam conservados no território da União, inviabilizando, deste modo, qualquer fiscalização, por entidade independente, expressamente exigida na Carta, pelo art. 8.º, n.º 3, do cumprimento das exigências de proteção e de segurança.

Face a todos os argumentos esgrimidos concluíram que "*há que considerar que, ao adotar a Diretiva 2006/24, o legislador da União excedeu os limites impostos pelo respeito do princípio da proporcionalidade à luz dos artigos 7.°, 8.° e 52.°, n.° 1, da Carta*". E declararam que "***[A] Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE, é inválida.***"

Por força da declaração de invalidade da Diretiva que originou a Lei n.º 32/2008 esta mantém-se em vigor mas poderá ser alvo de fiscalização da constitucionalidade em face do Primado do Direito da UE sobre os direitos nacionais.[18] Efetivamente a decisão do TJUE que considera inválido um ato de Direito secundário (neste caso a Diretiva de retenção de dados) porque viola o Direito primário tem um efeito *erga omnes*, traduzindo-se em consequências para todos: para todos os tribunais e demais aplicadores do direito que não podem mais aplicar um ato que viola direito superior; para o legislador que fica obrigado a eliminá-lo da ordem jurídica.[19] Donde, a decisão do TJUE constitui fundamento suficiente para que os tribunais

18 Tal já sucedeu em diversos países da UE, tendo as leis de transposição desta Diretiva sido consideradas inconstitucionais. Nomeadamente: Tribunal Constitucional da Roménia (Decisão n.º 1258, de 8 de outubro de 2009); Tribunal Constitucional da Alemanha (Sentença n.º 10/2010, de 2 de março); Tribunal Constitucional da República Checa (Sentença Pl. ÚS 24/10, de 31 de março de 2011).

19 Tende aqui a aceitar-se a primazia do direito da UE originário e derivado sobre o direito constitucional nacional, embora não deixe de se chamar a atenção para o facto de que se trata de um fenómeno material e funcionalmente limitado. (...) Na verdade, nas Declarações Relativas a Disposições dos Tratados, aprovadas quando da entrada em vigor do Tratado de Lisboa, encontra-se a Declaração 17, sobre o primado do direito comunitário, em que se lembra expressamente que, em conformidade com a jurisprudência do TJUE, os Tratados e o direito adotado pela União com base nos Tratados primam sobre o direito dos Estados membros, nas condições estabelecidas pela referida jurisprudência, tendo juntado inclusivamente um Parecer do Serviço Jurídico do Conselho afirmando que se trata aí de salvaguardar um princípio do direito comunitário. *Loc. cit.* pp. 67 a 69 *in* JÓNATAS E. M. MACHADO, *Direito da União Europeia*, 2.ª Edição, Coimbra Editora, 2012. Neste sentido, também, MARIA ROSA OLIVEIRA TCHING, "Juiz Natural – Um juiz cada vez mais europeu", *Revista Julgar*, n.º 14, Coimbra Editora, 2011, pp. 135-155.

nacionais dos Estados membros se abstenham de aplicar o ato considerado nulo e de reenviar a questão da respetiva validade para o TJUE.[20]

Sem este precioso e indispensável instrumento de identificação a prova digital fica seriamente comprometida e por mais que exista legislação, os crimes cometidos através da Internet deixarão de ser imputados a um determinado autor, por falta de elementos que conduzam até este e, consequentemente, ficará incólume à ação da justiça.[21]

20 *Loc. cit.* JÓNATAS MACHADO, *Ob. Cit.*. pp. 647-648

21 A este respeito remetemos para a nossa monografia *A Prova Digital em Processo Penal: o correio eletrónico*, Chiado Editora, 2.ª Edição, 2017, em especial para as páginas 93 a 99.

4. A CONEXÃO ENTRE A LEGISLAÇÃO ATUAL E A INVESTIGAÇÃO DA CIBERCRIMINALIDADE

Do que temos vindo a discorrer não restam dúvidas que a investigação criminal sai fragilizada face às normas legais que possuímos. Efetivamente a obtenção de prova é fulcral para que num processo-crime se possa imputar a responsabilidade penal ao agente. Caso contrário a prova sucumbe, por ter sido ilícita ou obtida tardiamente, e o arguido não ser condenado, por inexistência de provas.

Dos diversos problemas já enumerados iremos aflorar dois, para os quais ainda não dedicamos a atenção devida e por serem fulcrais na investigação da cibercriminalidade.

Primus, a equiparação da apreensão do correio eletrónico ao regime da correspondência do Código de Processo Penal. É sabido que nos dias que correm o uso regular do correio eletrónico é uma banalização. Eventualmente já o era há 10 anos, aquando da criação da lei do cibercrime, mas atualmente, e com a facilidade com que se pode efetuar um registo de correio eletrónico, é um dos problemas que afetam a investigação criminal a referida equiparação. Já o defendemos no passado[22] e continuamos a advogar que esta equiparação é inimiga de uma célere investigação. Proceder formalmente à equiparação do regime da correspondência, levando ao conhecimento do JIC os *e-mail's* apreendidos para que seja o primeiro a tomar conhecimento, leva a o JIC não leia todos os *e-mail* e não determine quais os que são de interesse para juntar aos autos. Antes leva o juiz a efetuar um despacho genérico delegando na Polícia a faculdade de ver os *e-mail's* e posterior junção dos que tenham interesse com a investigação. O espírito do legislador aquando da criação da norma do art. 179.º do CPP foi a da proteção da reserva da vida privada e familiar em observância da norma constitucional do art. 26.º, n.º 1 da CRP. Procedendo como se tem vindo a assistir, ou seja o JIC tomar conhecimento dos *e-mail*, mas não visualizando o seu conteúdo e delegando no OPC a faculdade de em primeira instância ver e juntar aos autos as mensagens de correio eletrónico, não só está a ser violado o regime processual penal como se está a permitir a divulgação de e-mail's com conteúdo da vida íntima dos visados por outras pessoas. PAULO PINTO DE ALBUQUERQUE afirma categoricamente que "*a omissão do exame da correspondência pelo juiz constitui uma nulidade do art. 120.º, n.º 2, alínea d), porque se trata de um acto processual legalmente obrigatório*"[23].

Concordamos com Rui Cardoso quando afirma que "*o legislador deveria então ter criado um regime autónomo e auto-suficiente, com repartição equilibrada de competências entre o Ministério Público e o juiz de instrução, a este reservando o estritamente necessário à*

22 ARMANDO DIAS RAMOS, *A prova digital em processo penal: o correio eletrónico*, 2.ª Edição, Chiado Editora, 2017.

23 In comentário ao art. 179, nota 12, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção dos Direitos do Homem*, 2.ª Edição, Universidade Católica Editora, 2008, p. 495.

garantia de direitos dos visados, adequado às especificidades técnicas das comunicações eletrónicas, muito diferentes da correspondência corpórea"[24].

Em nosso modesto entendimento o Ministério Público deveria delegar no investigador a faculdade de visualizar o conteúdo e selecionar os *e-mail's* de interesse, sendo este o único a visualizar o conteúdo dos mesmos e submetendo ao seu escrutínio a junção dos relevantes ao processo. Posteriormente, tal como sucede no regime das interceções telefónicas, o MP remeteria ao JIC para validação formal.

Secundus, o uso das ações encobertas na investigação da cibercriminalidade. O legislador previu, no n.º 2 do art. 19.º da Lei do Cibercrime, o recurso a meios e dispositivos informáticos, nas ações encobertas, observando-se a utilização das regras previstas no CPP relativas à interceção das comunicações. Analisando as regras do CPP que dizem respeito às escutas telefónicas, ínsitas nos artigos 187.º a 189.º, verificamos que não obtemos respostas a certas perguntas, as quais fazem parte do nosso problema. Desde logo porque a função do agente encoberto não se reconduz a uma mera interceção. Como bem já referimos noutras instâncias[25], intercetar significar intrometer de permeio, ou seja, entre o emissor e o recetor alguém consegue captar todo o conteúdo das comunicações eletrónicas. Ora, salvo melhor opinião em contrário, não nos encontramos perante a figura do agente encoberto. Define a Lei das Ações Encobertas, no n.º 2, do art. 1.º, que se consideram ações encobertas aquelas que sejam desenvolvidas por funcionários de investigação criminal ou por terceiros, atuando sob controlo da Polícia Judiciária, para prevenção ou repressão dos crimes (...), com ocultação da sua qualidade e identidade (negrito nosso). É certo que quando se efetua uma interceção telefónica, regime previsto no CPP, para onde somos levados obrigatoriamente pelo legislador na Lei do Cibercrime, não existe qualquer ocultação da qualidade do agente ou da sua identidade, apenas se trata de um procedimento técnico em que se consegue "escutar" a comunicação, seja ela telefónica ou de dados informáticos. Subjazem, pois, muitas dúvidas como se poderá efetivamente aplicar o art. 19.º da Lei do Cibercrime às regras enunciadas no CPP. Recorrendo a DÁ MESQUITA "*consagra-se uma norma espúria no ordenamento jurídico português ao prever, sem qualquer outro enquadramento, o "recurso a meios e dispositivos informáticos" em ações encobertas*"[26].

Os problemas, para além destes que já enunciamos, são mais diversos e complexos, os quais a legislação não dá resposta, por nos encontrarmos num estado avançado da tecnologia e do direito continuar estagnado. O legislador continua ainda a olhar para a criminalidade informática, que pode ser muito grave, inclusive com atos terroristas, com olhos de equiparação entre duas realidades que são bem distintas.

---

24 RUI CARDOSO, "Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei 109/2009, de 15.IX", In *Revista do Ministério Público*, n.º 153.º, Janeiro-Março de 2018, Almedina, p. 178.

25 Ver nosso *A prova digital em processo penal...*, p. 52.

26 PAULO DÁ MESQUITA, *Processo Penal, Prova e Sistema Judiciário*, Coimbra Editora, 2010, p. 127.

Um dos problemas que desde já se coloca é se será lícito a um investigador ou terceiro, na qualidade de agente infiltrado, enviar *benware*[27], sob a forma de disfarce de atualização de um *software* ou por intermédio de qualquer outro subterfúgio, para poder aceder a todo o conteúdo do disco rígido do computador do suspeito? Constata-se que efetivamente numa ação encoberta relativa a tráfico de estupefacientes, por exemplo, o agente que se infiltra numa determinada zona e convive com os suspeitos detém uma perceção visual do espaço que o rodeia. Poderá assim confirmar a existência de balanças de precisão, de panfletos prontos a serem utilizados, etc., ou de outros elementos tidos por pertinentes para os fins da investigação em curso. E estes elementos, ainda que o agente não visualize diretamente o produto estupefaciente, são tidos em linha de conta para a investigação e poderão concatenar as provas de modo a que existam fundadas suspeitas ou indícios suficientes dos crimes que ali se praticam. E quem se refere a crimes de narcotráfico também se reconduz a crimes de terrorismo, com a perceção de elementos que possam originar um ataque em massa ou de grandes proporções. A nível informático tal situação não é assim tão linear. Quanto muito o suspeito, após ter ganho a confiança do seu interlocutor, poderá permitir apenas o acesso a uma pasta partilhada do seu computador ou servidor, ficando o agente maniatado de obter outros elementos que poderão conduzir a provas irrefutáveis da prática de crimes cibernéticos tais como de (ciber)terrorismo ou de financiamento dos mesmos, entre outros.

Assim, coloca-se novo problema, será lícito a um agente infiltrado criar artefactos virtuais, sem entrar na esfera da provocação, de forma a "atrair" e identificar criminosos? A este respeito não poderemos esquecer a criação da menina virtual, apelidada de *Sweetie*, de origem filipina e com 10 anos de idade, pela ONG holandesa *Terre des Hommes*[28], onde foram identificados em 2013, durante 10 semanas em que colocaram a imagem virtual da menina em salas de conversação (denominados *chats*) de pornografia infantil, mais de 1.000 homens interessados em ter sexo com menores de 16 anos. Onde efetivamente termina a ação encoberta e começa a ação provocadora no ciberespaço?

Será lícito criar perfis falsos nas redes sociais, sem conhecimento das autoridades judiciárias e consequentemente à margem do regime de agente infiltrado, para obter mais informações do suspeito, incluindo-se aqui a interação virtual com os suspeitos?

O mesmo se reconduz aos crimes de terrorismo, sejam estes praticados de forma tradicional, sejam praticados através da Internet. O agente encoberto poderá com a utilização de técnicas informáticas entrar na esfera privada do suspeito e obter informações que não conseguiria de outro modo?

---

27 Por opisição a *Malware* , i.é, nome abreviado para "software malicioso". *Malware* é qualquer tipo de software indesejado, instalado sem o seu devido consentimento. Vírus, *worms* e *cavalos de tróia* são exemplos de *software* mal-intencionado que com frequência são agrupados e chamados, coletivamente, de *malware*. In http://www.microsoft.com/pt-br/security/resources/malware-whatis.aspx [*acedido em 5 de julho de 2019*].
28 http://www.terredeshommes.nl/languages/en [*acedido em 5 de julho de 2019*].

Não almejamos responder a todas estas perguntas, face à complexidade que as mesmas abarcam e por nos conduzirem a outro campo de outra importância, que se relaciona com Direitos, Liberdades e Garantias dos cidadãos.

É na Constituição da República que encontramos o expoente máximo da garantia dos cidadãos no que aos seus Direitos e Liberdades dizem respeito, podendo existir uma contração destes em situações previstas na Lei e sempre em obediência aos princípios da necessidade, subsidiariedade e proporcionalidade (art. 18.º CRP).

As ações intrusivas, na vida pessoal e familiar, provocadas pela figura do agente encoberto digital, ao conseguir aceder aos conteúdos do computador do visado, a conseguir localizar de forma imediata a sua localização, através do sistema GPS, revelam-se menores face aos atos que poderão a vir ser cometidos, salvaguardando-se, através da prevenção, a vida de muitas pessoas, entre outros bens jurídicos.

Urge mudar este paradigma para que, dentro da legalidade, seja possível realizar investigações criminais que salvaguardem os direitos e as liberdades dos suspeitos. Por outro lado, muitas das investigações ficam inquinadas porque adotado o regime das interceções das comunicações a dados encriptados os investigadores não lograram obter quaisquer informações por força da codificação destas.

5. EM JEITO DE CONCLUSÃO

Do decurso do tempo, nestes 10 anos, de aplicação da lei do cibercrime verifica-se um fosso abismal entre a legislação em vigor e a tecnologia existente.

Como discorremos as tecnologias informáticas estão evoluídas e surgem novos ilícitos criminais que não poderão ser investigados por falta de norma legal. A título de exemplo a criação de perfis falsos nas redes sociais, usando fotografias e criando a ilusão que se trata de uma pessoa conhecida de terceiros, com intuitos ilícitos. De igual modo a criação de endereços de correio eletrónico[29] usurpando a identidade de terceiros é outro dos problemas que urge tipificar. Se é certo que o art. 3.º da lei do cibercrime poderá acolher esta situação, quando utilizados para finalidades juridicamente relevantes tal não sucede quanto à criação do próprio endereço de *e-mail* pois não se está, com intenção, a introduzir, modificar, apagar ou suprimir dados informáticos, nem a interferir num tratamento de dados informáticos. De igual modo não se produzem dados ou documentos não genuínos.

A lei do cibercrime necessita de uma adaptação a esta realidade mormente no âmbito da recolha de prova. O uso corriqueiro do correio eletrónico e a implementação de sistemas encriptados conduz-nos a outra era dos crimes informáticos.

Urge adaptar ao direito interno a Diretiva 2013/40/UE, pois a mesma encerra medidas de investigação mais célere com as congéneres europeias, nomeadamente:

1.º - Aproximando o direito penal dos Estados-Membros no domínio dos ataques contra os sistemas de informação, estabelecendo um conjunto de regras mínimas relativamente às infrações penais e às suas sanções;

2.º - A utilização de *botnets*[30] para fins criminosos, que coloca em causa sistemas de informações de infraestruturas críticas da União, comprometendo a realização de uma sociedade de informação mais segura e de um espaço de liberdade, segurança e justiça; e,

29 Se considerarmos os endereços dos servidores de webmail verifica-se a panóplia de possibilidade de criação de endereços de e-mail semelhantes.

30 Na própria exposição de motivos encontramos a definição de *botnet*. Assim, "*o termo «botnet» designa uma rede de computadores que foram infectados por software maligno (vírus informáticos). Esta rede de computadores «sequestrados» («zombies») pode ser ativada para executar ações específicas, como atacar sistemas de informação (ciberataques). Estes «zombies» podem ser controlados – frequentemente sem o conhecimento dos utilizadores dos computadores «sequestrados» – por outro computador, igualmente conhecido como «centro de comando e de controlo». As pessoas que controlam este centro fazem parte dos infractores, já que utilizam os computadores «sequestrados» para lançar ataques contra os sistemas de informação. É muito difícil localizar os autores da infracção, dado que os computadores que formam o «botnet» e realizam o ataque podem encontrar-se num local diferente daquele em que se encontra o infractor.*" Disponível *online* em http://new.eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX%3A32013L0040&qid=1377248567337 [*acedido em 14 de agosto de 2019*].

3.º - Aumenta a eficácia dos pontos de contato 24/7, responsáveis pela aplicação da lei nos Estados-Membros, com respostas urgentes a terem que ser obtidas no prazo de 8 horas.

Não será necessário aos órgãos de investigação o recurso a meios informais para obtenção de informação se se tivesse uma cooperação internacional mais eficaz. A nível interno a obtenção de elementos de prova poderia também ser mais célere se o titular da ação penal (Ministério Público) detivesse mais poder e apenas a intervenção do JIC fosse requerida aquando da hipotética violação de direitos fundamentais, no seu núcleo (ou o conteúdo) essenciais[31].

Só desta forma, a par de um reforço na justiça com a dotação de magistrados com mais conhecimentos informáticos e mais recursos humanos e técnicos nas polícias, se logrará a eficácia do combate ao cibercrime. Na verdade, assistimos a uma deslocação do mundo criminal para o mundo virtual, no qual os meliantes trocaram a insegurança pela segurança, a possibilidade de ser identificado com a certeza da quase anonimização, a punição pelo sentimento de impunidade.

31 GOMES CANOTILHO/VITAL MOREIRA, *Constituição da República Portuguesa Anotada*, I, 4.ª ed., Coimbra, 2007, p. 153

6.BIBLIOGRAFIA

ALBUQUERQUE, PAULO PINTO DE, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção dos Direitos do Homem*, 2.ª Edição, Universidade Católica Editora, 2008.

BRAZ, JOSÉ, *Investigação Criminal, a organização, o método e a prova, Os desafios da nova criminalidade*, Almedina, 2009.

CANOTILHO, J. J. GOMES; MOREIRA, VITAL, *Constituição da República Portuguesa Anotada*, I, 4.ª ed., Coimbra, 2007.

CARDOSO, RUI, "Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei 109/2009, de 15.IX", In *Revista do Ministério Público*, n.º 153.º, Janeiro-Março de 2018, Almedina.

MACHADO, JÓNATAS E. M., *Direito da União Europeia*, 2.ª Edição, Coimbra Editora, 2012

MESQUITA, PAULO DÁ, *Processo Penal, Prova e Sistema Judiciário*, Coimbra Editora, 2010.

NUNES, DUARTE RODRIGUES, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, Gestlegal, 2018.

RAMALHO, DAVID SILVA, "A investigação criminal na Dark Web", in *Revista da Concorrência e Regulação*, n.º 14/15, Almedina, 2013.

RAMOS, ARMANDO DIAS, "A novíssima Diretiva relativa ao cibercrime", In SOUSA, CONSTANÇA URBANO DE (Coord.), *O Espaço de liberdade, segurança e justiça da UE: desenvolvimentos recentes*, EDIUAL, Lisboa, maio de 2014.

RAMOS, ARMANDO DIAS, *A prova digital em processo penal: o correio eletrónico*, 2.ª Edição, Chiado Editora, 2017.

TCHING, MARIA ROSA OLIVEIRA, "Juiz Natural – Um juiz cada vez mais europeu", *Revista Julgar*, n.º 14, Coimbra Editora, 2011

VERDELHO, PEDRO, "Cibercrime", in *Dicionário da Sociedade de Informação*, IV, Coimbra Editora, 2003.

VERDELHO, PEDRO, "A Convenção sobre o Cibercrime do Conselho da Europa – Repercussões na Lei Portuguesa", in *Direito da Sociedade da Informação*, VI, Coimbra Editora, 2006.

O FENÓMENO DO *RANSOMWARE* E O SEU ENQUADRAMENTO JURÍDICO-PENAL

DUARTE RODRIGUES NUNES [1]

1 Juiz de Direito. Doutor em Direito pela Faculdade de Direito da Universidade de Lisboa. Investigador integrado do CIDPCC e não integrado do CIJIC. Endereço eletrónico: duarterodriguesnunes@hotmail.com.

ABSTRACT

Ransomware is a type of malware that aims to prevent the victim from accessing computer systems and/or data through encryption and then require a ransom to be decrypted and to recover access to the data. Ransomware can be considered as a type of malware and as a criminal activity.

Portuguese Law does not have a specific incrimination of Ransomware, so we must try to subsume the conduct to any crime provided by Law.

In this article we will try to determine which crimes are committed by criminals in connection with this criminal activity.

Keywords: Ransomware; Cybercrime; Illegal access; Data interference; Extortion.

RESUMO

O *Ransomware* é um tipo de *malware* desenvolvido com a finalidade de o agente impedir a vítima de aceder a sistemas e/ou a dados informáticos mediante a encriptação de dados informáticos para, seguidamente, exigir o pagamento de um resgate para serem desencriptados e a vítima recuperar o acesso aos dados. O *Ransomware* pode ser considerado enquanto tipo de *malware* e enquanto atividade criminosa.

O Direito português não possui uma incriminação específica do *Ransomware*, havendo que tentar subsumir a conduta do agente a algum dos tipos de crime previstos na lei.

Neste artigo, tentar-se-á determinar quais os crimes que são cometidos pelos criminosos no âmbito desta atividade criminosa.

Palavras-chave: *Ransomware*; Cibercrime; Acesso ilegítimo; Dano relativo a programas outros dados informáticos; Extorsão.

Sumário: 1. Introdução. 2. O conceito de *Ransomware*. 3. O acesso ilegítimo ao sistema informático e aos dados informáticos alheios. 4. O impedimento de o titular aceder aos dados e o (eventual) entravamento do sistema informático. 5. A exigência e o pagamento do resgate. 6. Conclusões. Bibliografia. Jurisprudência.

1.INTRODUÇÃO

Como enfatiza a ONU, o Cibercrime[1] é uma forma de crime transnacional em evolução. O Cibercrime é também uma realidade complexa, decorrendo a sua complexidade do facto de ocorrer no território sem fronteiras do Ciberespaço (em que os agentes e as vítimas podem estar situados em países diversos e os efeitos da prática dos crimes produzir-se em todo o Mundo) e do crescente envolvimento de organizações criminosas, gerando a necessidade de criar uma resposta urgente, dinâmica e internacional[2]. Segundo a Europol[3], o *Ransomware* é, atualmente, a atividade criminosa mais frequente ao nível dos ataques de *malware* cuja finalidade passa por obter lucro, superando inclusivamente os *Banking Trojans*[4].

Nos Estados Unidos, o *U.S. Federal Trade Commission* (FTC) considera o *Ransomware* como uma das ciberameaças mais perigosas para as pessoas e para as empresas e como a forma de *malware* mais lucrativa para os criminosos. Por seu turno, o FBI constituiu um grupo de trabalho especial para combater o *Ransomware*[5].

O vocábulo *Ransomware* resulta da aglutinação das palavras inglesas *ransom* (resgate) e *software* (programa). Tal designação surgiu devido à peculiaridade de sua atuação nos

1 Definimos Cibercrime como «*o facto tipificado na lei como crime que é praticado através da utilização de um sistema informático na aceção do art. 2.º, al. a), da Lei n.º 109/2009 ou em que o sistema informático é o objeto da ação, ainda que como alvo simbólico, ou dito de o outro modo, o facto tipificado na lei como crime em que o sistema informático é objeto ou instrumento do crime ou cujo cometimento está significativamente ligado à utilização de um sistema informático*» [cfr. DUARTE RODRIGUES NUNES,
Os meios de obtenção de prova previstos na Lei do Cibercrime, pp. 13-14 (nota 1)].

2 *Vide* www.unodc.org/unodc/en/cybercrime/index.html (acedido em 11/06/2018).

3 EUROPOL, IOCTA, 2018, p. 7, *in www.europol.europa.eu/activities-services/main-reports/internet-organised-crimethreat-assessment-iocta-2018* (acedido em 08/06/2019).

4 Os *Banking Trojans* são um *malware* do tipo Cavalo de Troia que se "disfarça" de aplicativo ou de *software* genuíno que os utilizadores baixam e instalam ou, aberto o *e-mail* que o contém, se instala sub-repticiamente no sistema informático-alvo. Uma vez instalados, os *Banking Trojans* permitem o acesso dos agentes do crime a dados bancários, usualmente para levar a cabo atividades de *Phishing*.

5 Cfr. JAMES A. SHERER/MELINDA L. MCLELLAN/EMILY R. FEDELES/NICHOLE L. STERLING, "Ransomware – Practical and legal considerations for confronting the new economic engine of the dark web", *in* Richmond Journal of Law & Technology, Volume XXIII, Fascículo 3, pp. 1-2, *in* https://jolt.richmond.edu/files/2017/04/Sherer-Final-May-1.pdf (acedido em 13/06/2019).

dispositivos informáticos. O *Ransomware* fez surgir as expressões sequestro de dados (ato de bloquear, inutilizar ou inviabilizar o acesso à dados) e extorsão digital ou criptoviral (ato de solicitar vantagem ilícita/pagamento em troca da liberação dos dados). Esta ameaça cibernética ganhou grande destaque no cenário internacional, sendo considerada a ameaça cibernética mais rentável para a cibercriminalidade.

O primeiro *Ransomware* (AIDS) de que há notícia surgiu em 1989, tendo sido desenvolvido por Joseph Popp, um biólogo evolucionista. O AIDS (*Aids Info Disk* ou *PC Cyborg Trojan*) atuava durante a nonagésima inicialização do sistema operacional após o AIDS ter sido instalado no dispositivo, criptografando os dados e tornando o sistema inutilizável. De seguida, era enviado à vítima um alerta para a renovação de licença, exigindo o pagamento de uma quantia à corporação PC Cyborg para que a vítima pudesse retomar o acesso aos dados. Como o AIDS criptografava os nomes dos arquivos utilizando criptografia simétrica (par de chaves iguais), uma vez descoberto o segredo, foi relativamente simples reverter o processo e identificar o autor, o que ocorreu após a análise do código por especialistas em segurança da informação. Popp foi preso pela *New Scotland Yard* e condenado numa pena de prisão[6].

Posteriormente, surgiram novos tipos de *Ransomware* como o *Gpcode, Archiveus, Krotten, Cryzip, MayArchive*. Como referimos, o *Ransomware* é uma realidade em constante evolução[7], permitindo aos criminosos superar as medidas de proteção que vão sendo utilizadas pelas vítimas e a sua ameaça aumentou exponencialmente com o surgimento de um modelo de negócio que facilitou o acesso ao *Ransomware* por qualquer criminoso que pretenda utilizá-lo nas suas atividades criminosas (sendo vendido na Internet a preços bastante acessíveis,

6 Cfr. RENAN CABRAL SAISSE, **Ransomware: "sequestro" de dados e extorsão digital, in** *http://direitoeti.com.br/artigos/Ransomware-sequestro-de-dados-e-extorsao-digital/* (acedido em 11/06/2019).

7 O *Ransomware* atinge todo o tipo de dispositivos que utilizem a Internet (computadores, *tablets*, *smartphones*), bem como a "Internet das coisas" (sistemas de controle industrial, refrigeradores, sistemas de tratamento de doentes, etc.) [cfr. JAMES A. SHERER/MELINDA L. MCLELLAN/EMILY R. FEDELES/NICHOLE L. STERLING, "Ransomware – Practical and legal considerations for confronting the new economic engine of the dark web", *in* Richmond Journal of Law & Technology, Volume XXIII, Fascículo 3, p. 15, *in https://jolt.richmond.edu/files/2017/04/Sherer-Final-May-1.pdf* (acedido em 13/06/2019)].

De acordo com TERRENCE AUGUST/DUY DAO/MARIUS FLORIN NICULESCU, Economics of Ransomware Attacks, p. 1, *in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3351416* (acedido em 13/06/2019), e MASARAH PAQUET-CLOUSTON/BERNHARD HASLHOFER/BENOÎT DUPONT, "Ransomware payments in the Bitcoin ecosystem", *in* Journal of Cybersecurity, 2019, p. 1, *in https://watermark.silverchair.com* (acedido em 13/06/2019), o aumento exponencial do *Ransomware* deveu-se ao desenvolvimento da criptografia, à possibilidade de anonimização através da utilização da *Dark Web* e de mecanismos como o TOR e ao incremento dos pagamentos em criptomoedas.

permitindo a utilização também por indivíduos com menores aptidões em termos informáticos e estando, por isso, acessível a todos os escalões de cibercriminosos)[8].

De acordo com a Europol[9], assistiu-se, em 2017[10], a uma diminuição do crescimento do *Ransomware*, que, contudo, continuava a superar os *Banking Trojans* ao nível dos ataques de *malware* cuja finalidade passa pela obtenção de lucro, tendência que se estima continuar nos próximos anos. Ainda segundo a Europol[11], os ataques de *Ransomware WannaCry* e *NotPetya*, ocorridos em meados de 2017, foram executados a uma escala global sem precedente, afetando cerca de 300.000 vítimas em 150 países e causando, só o *WannaCry*, um prejuízo económico total de cerca de 4 biliões de dólares americanos (USD) (estimando-se que, em 2017, o total dos prejuízos causados por ataques de *Ransomware* ascendeu a mais de 5 biliões de USD); na União Europeia, tais ataques afetaram um amplo âmbito de indústrias e infraestruturas críticas, incluindo serviços de saúde, telecomunicações, transportes e indústrias de manufatura; ainda em 2017, o *Ransomware Bad Rabbit* atingiu mais de 200 vítimas na Rússia e na Europa Oriental, afetando infraestruturas críticas nos setores da saúde, transportes e finanças.

Nalguns países, os ataques de *Ransomware* são tendencialmente aleatórios, atingido, ora cidadãos ora empresas, indiciando que se trata de criminosos "desorganizados"; todavia, noutros países, os ataques tendem a ser direcionados contra pessoas ou empresas específicas, o que indicia que se trata de crime organizado.

O *Ransomware*, pelo seu potencial altamente lucrativo e pela acessibilidade dos instrumentos cuja utilização requer, é levado a cabo por criminosos "individuais", por

---

8 Cfr. JAMES A. SHERER/MELINDA L. MCLELLAN/EMILY R. FEDELES/NICHOLE L. STERLING, "Ransomware – Practical and legal considerations for confronting the new economic engine of the dark web", *in* Richmond Journal of Law & Technology, Volume XXIII, Fascículo 3, pp. 2, 14-15 e 17-18, , *in* *https://jolt.richmond.edu/files/2017/04/Sherer-Final-May-1.pdf* (acedido em 13/06/2019).

9 EUROPOL, IOCTA, 2018, p. 7, *in www.europol.europa.eu/activities-services/main-reports/internet-organised-crimethreat-assessment-iocta-2018* (acedido em 08/06/2019).

Também o Relatório de Ameaças à Segurança na Internet (ISTR) de 2019 da Symantec nos dá nota de que, durante o ano de 2018, o número de infeções de *Ransomware* caiu 20% em relação a 2017 [cfr. A atividade de *Ransomware* diminuiu, mas ele ainda é uma ameaça perigosa, *in* *https://www.symantec.com/blogs/portugues/atividade-ransomware-diminuiu-ainda-ameaca-perigosa* (acedido em 17/07/2019)].

No entanto, em 2016, de acordo com o Relatório anual de ameaças da SonicWall, o *Ransomware* crescera 167 vezes, passando de um total de 3,8 milhões de ataques em 2015 para 638 milhões em 2016 [cfr. Cibercriminosos mudam foco e ransomware cresce 167 vezes em 2016, *in http://computerworld.com.br/cibercriminosos-mudam-foco-e-ransomware-cresce-167-vezes-em-2016* (acedido em 04/07/2018)] e 2017 fora o ano dos devastadores ataques do *WannaCry* e do *NotPetya*.

10 No momento em que escrevemos o presente artigo, o IOCTA 2019 (relativo ao ano de 2018 ainda não está disponível).

11 EUROPOL, IOCTA, 2018, p. 16, *in www.europol.europa.eu/activities-services/main-reports/internet-organised-crimethreat-assessment-iocta-2018* (acedido em 08/06/2019).

organizações criminosas "tradicionais" (para obtenção de lucro), por organizações terroristas (para financiamento das suas atividades terroristas) e até por Estados (para fins de guerra cibernética e também - sobretudo no caso da Coreia do Norte - de financiamento de determinados programas, *maxime* programas de armamento)[12].

Existem alvos preferenciais para o *Ransomware* como o setor da saúde (hospitais e clínicas, que tendem a pagar imediatamente o resgate exigido, pelos riscos que a privação do acesso ao sistema ou aos dados acarreta para os pacientes), empresas altamente dependentes do uso de sistemas informáticos, advogados[13] e sistemas informáticos em que sejam guardados ou que permitam aceder a *big data* armazenados na nuvem[14].

De acordo com a EUROPOL[15], baseando-se nas informações provenientes das empresas do ramo da informática e das autoridades públicas que se ocupam da prevenção/repressão do Cibercrime, fruto das receitas que proporciona aos criminosos e da acessibilidade dos meios necessários para o levar a cabo, o *Ransomware* continuará a florescer, embora existam algumas previsões de que possa vir a ser ultrapassado pela mineração de

12 Dois exemplos dessa realidade são o ataque cibernético não reivindicado pela Rússia contra a Estónia em 2007 (que paralisou vários sites governamentais estónios durante algumas horas) e o ataque cibernético, com utilização do vírus *Stuxnet* (cuja produção se suspeita ter sido ordenada pelos Estados Unidos e/ou Israel) a uma central nuclear iraniana em 2010, onde se produzia urânio enriquecido. Em ambos os casos, estamos perante as chamadas Ciberarmas, usualmente utilizadas por países e não tanto por Cibercriminosos "particulares", embora nada impeça que, num segundo momento, esse *malware* seja utilizado por estes (nomeadamente organizações terroristas para cometerem atos de Ciberterrorismo).

Do mesmo modo, existem fortes suspeitas de que o regime norte-coreano leva a cabo atividades de Cibercrime como forma de obter financiamento para os seus programas de armamento (*v.g.* através de um ataque de *Spear Phishing* contra o Banco Central do Bangladesh, em que terão sido roubados 81 milhões de dólares americanos) e como forma de guerra cibernética contra outros Estados ou empresas considerados inimigos; assim, o regime norte-coreano tem sido acusado (embora negando sempre tais acusações) de roubar *e-mails*, de ameaçar a Sony Pictures com ataques cibernéticos no caso de um filme de comédia satírica que retratava uma tentativa de assassinato de Kim Jong-un ir para o ar (o filme acabou por não ser lançado) e de tentar entrar nos sistemas informáticos da Lockheed Martin (uma empresa que fornece componentes de defesa aérea ao Governo dos Estados Unidos), bem como de outras empresas dos setores da defesa, finanças, energia, telecomunicações e saúde, existindo igualmente suspeitas de que, em 2017, os norte-coreanos se aproveitaram do ataque do *WannaCry* para realizarem ações de sabotagem contra hospitais no Reino Unido, o sistema ferroviário na Alemanha e o sistema de redes de comunicações móveis de Espanha.

De resto, na sequência do ataque Cibernético à Estónia, os Estados Unidos criaram um quinto domínio na sua doutrina militar: o Ciberespaço (os outros quatro são a Terra, o ar, o mar e o Espaço) (cfr. MISHA GLENNY, Darkmarket, pp. 216-217).

13 Cfr. JAMES A. SHERER/MELINDA L. MCLELLAN/EMILY R. FEDELES/NICHOLE L. STERLING, "Ransomware – Practical and legal considerations for confronting the new economic engine of the dark web", *in* Richmond Journal of Law & Technology, Volume XXIII, Fascículo 3, pp. 20-22, *in* *https://jolt.richmond.edu/files/2017/04/Sherer-Final-May-1.pdf* (acedido em 13/06/2019).

14 Cfr. DAVID WALL, "How big data feeds big crime", *in* Global History: A Journal of Contemporary World Affairs, 2018, p. 31, *in* *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3359972* (acedido em 12/06/2019)

15 EUROPOL, IOCTA, 2018, p. 26, *in* *www.europol.europa.eu/activities-services/main-reports/internet-organised-crimethreat-assessment-iocta-2018* (acedido em 08/06/2019). A visão da EUROPOL é também partilhada pela empresa Kaspersky Lab [cfr. Kaspersky lança três previsões sobre as ameaças para as criptomoedas em 2019, *in* *https://wintech.pt/w-news/26233-kaspersky-lanca-tres-previsoes-sobre-as-ameacas-para-as-criptomoedas-em-2019* (acedido em 14/07/2019)].

criptomoedas[16] (*Cryptocurrency Mining*) como a maior ameaça à Cibersegurança, uma vez que se trata de uma atividade muito mais atrativa para os cibercriminosos, por exigir pouco ou nenhum envolvimento de vítimas e, pelo menos atualmente, pouca atenção das autoridades (dado que a mineração de criptomoedas, em si mesma, não é ilegal). No fundo, tendo em conta os valores que as criptomoedas têm atingido (especialmente o *Bitcoin*), a mineração de criptomoedas é suscetível de proporcionar lucros mais elevados do que o *Ransomware* e, atualmente, não envolve ou, quando muito, envolve "riscos penais" menores do que o *Ransomware*.

16 A mineração de criptomoedas consiste em validar as transações de outras pessoas com um computador e adicioná-las à *Blockchain*. Em troca, os criptomineiros (*Crypto Miners*) recebem criptomoedas. O problema desta atividade, aparentemente inócua, é que, para além de poder estar a ser prestado um auxílio a atividades de branqueamento de capitais e/ou de financiamento do terrorismo, do ponto de vista da Cibersegurança, poderá suceder que, para aumentarem a sua "produtividade", os criptomineiros se instalem maliciosamente numa rede informática (*v.g.* de uma empresa) previamente infetada, aí realizando uma mineração discreta, que é muito mais atrativa (por não chamar a atenção das autoridades e poder nem ser detetada pelos proprietários dessas redes) do que a exigência do pagamento de um resgate.

2. O CONCEITO DE *RANSOMWARE*

De acordo com MÁRIO ANTUNES/BALTAZAR RODRIGUES[17], um ataque de *Ransomware* «*consiste no acesso ilícito aos computadores de uma empresa, seguindo-se a posterior encriptação dos dados aí armazenados. De seguida, os atacantes iniciam a fase da extorsão à empresa, exigindo avultadas quantias em dinheiro para que os dados fiquem novamente acessíveis*».

Pela nossa parte, entendemos que o *Ransomware* deverá ser considerado sob duas perspetivas: como tipo de *malware* e como fenómeno criminoso ou atividade criminosa.

Enquanto tipo de *malware*[18], o *Ransomware* é um tipo de *malware* desenvolvido com a finalidade de o agente do crime ter acesso a sistemas informáticos e aos dados neles

---

17 MÁRIO ANTUNES/BALTAZAR RODRIGUES, Introdução à Cibersegurança, p. 127.

JAMES A. SHERER/MELINDA L. MCLELLAN/EMILY R. FEDELES/NICHOLE L. STERLING, "Ransomware – Practical and legal considerations for confronting the new economic engine of the dark web", *in* Richmond Journal of Law & Technology, Volume XXIII, Fascículo 3, p. 1, *in https://jolt.richmond.edu/files/2017/04/Sherer-Final-May-1.pdf* (acedido em 13/06/2019), definem *Ransomware* como «*um software malicioso que encripta os dados de um dispositivo ou um sistema e impede o acesso ou a recuperação desses dados até que proprietário pague um resgate*».

18 O *malware* (designação que resulta da aglutinação de sílabas das palavras inglesas *malicious* e *software* e que significa programa informático malicioso) é um programa informático que visa permitir a quem o utiliza infiltrar-se num sistema informático alheio, com o intuito de causar prejuízos ou de obter informações (confidenciais ou não), que, de outro modo, não poderia obter. O *malware* inclui uma miríade de tipos de programas, onde se incluem os vírus, *Worms* (vermes), "bombas lógicas", "cavalos de Troia", *keyloggers*, "programas *zombie*", *backdoors*, etc., podendo aparecer sob a forma de código executável, *scripts* de conteúdo ativo, etc.

Existem vários tipos de *Ransomware*. Assim, em primeiro lugar, encontramos o *Mobile Device Ransomware*, que infeta dispositivos Android através de falsas aplicações ou serviços populares, como um antivírus ou o *Adobe Flash*. O *modus operandi* deste tipo de *Ransomware* consiste em bloquear o ecrã e exigir um pagamento para o desbloquear de novo.

Um segundo tipo de *Ransomware* é o *Master Boot Record* (MBR) *Ransomware*, que vai atacar uma parte do disco rígido do computador [a *Master Boot Record* (MBR) que possibilita a inicialização do sistema operativo]. O MBR *Ransomware* altera a *Master Boot Record* do disco rígido, impedindo a inicialização normal e solicitando um código para a permitir, que, para ser obtido, impllicará o pagamento de um resgate.

Um terceiro tipo de *Ransomware* é o *Ransomware Encrypting Web Servers*, em que os dados armazenados em servidores *Web* são encriptados através do aproveitamento das vulnerabilidades dos sistemas de gestão de conteúdo *Web*.

Um quarto tipo de *Ransomware* é o *Lock Screen Ransomware*, que vai bloquear o ecrã do computador exibindo uma mensagem em que é exigido o pagamento de um resgate para que o ecrã seja desbloqueado.

Um outro tipo de *Ransomware* é o *Encryption Ransomware (Cryptolocker)*, que encripta todos os dados do computador (documentos, vídeos, fotografias, músicas, etc.).

Dada a enorme profusão deste tipo de *malware* e os enormes lucros que proporciona aos criminosos, existirão certamente outros tipos de *Ransomware*, mas estes serão, porventura, os mais disseminados. De resto, a EUROPOL, IOCTA, 2018, p. 16, *in www.europol.europa.eu/activities-services/main-reports/internet-organised-crimethreat-assessment-iocta-2018* (acedido em 08/06/2019), refere que, atualmente, há uma infinidade de tipos de *Ransomware*, sendo o *Cerber*, o *Cryptolocker, Crysis*, o *Locker Curve-Tor-Bitcoin (CTBLocker),* o *Dharma e* o *Locky* os mais reportados.

Por seu turno, JAMES A. SHERER/MELINDA L. MCLELLAN/EMILY R. FEDELES/NICHOLE L. STERLING, "Ransomware – Practical and legal considerations for confronting the new economic engine of the dark web", *in* Richmond Journal of Law & Technology, Volume XXIII, Fascículo 3, pp. 6 e ss., *in*

armazenados sem conhecimento do respetivo titular com o objetivo de encriptar os dados (criptografando-os ou compactando-os com senhas e, em muitos casos, inutilizando o próprio sistema infetado) e impedir o seu titular de lhes aceder para, posteriormente, exigir o pagamento de uma determinada quantia - usualmente em criptomoedas (sobretudo em *Bitcoin*, mas não só[19])[20] - para recuperação do acesso aos dados.

Enquanto fenómeno criminoso ou atividade criminosa, o *Ransomware*[21] consiste numa atividade que se consubstancia, numa primeira fase, no acesso ilegítimo a sistemas

---

https://jolt.richmond.edu/files/2017/04/Sherer-Final-May-1.pdf (acedido em 13/06/2019), e TERRENCE AUGUST/DUY DAO/MARIUS FLORIN NICULESCU, Economics of Ransomware Attacks, p. 1, *in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3351416* (acedido em 13/06/2019), entendem que existem apenas dois tipos de *Ransomware*: o *Locker Ransomware* e o *Crypto Ransomware.*

O *Locker Ransomware* consiste em restringir o acesso do utilizador aos sistemas infetados travando a *interface* ou os recursos de computação dentro do sistema e bloqueando o acesso ao computador ou aos dados; os dados armazenados no sistema informático mantém-se inalterados, limitando-se o criminoso a bloquear a "porta" (em sentido metafórico) que permite aceder-lhes e a exigir o pagamento de um regate para "destrancar" a "porta", podendo a vítima, em vez de pagar o resgate, tentar ignorar a "porta", perfurando a fechadura, retirando a "porta" das "dobradiças", removendo as "paredes" ao redor do conteúdo do sistema. Diversamente, o *Crypto Ransomware* encripta os dados armazenados no sistema informático infetado, continuando o sistema a poder ser utilizado pelo utilizador, que, no entanto, não pode aceder aos dados enquanto não pagar o resgate, sendo que o uso da encriptação tornará o acesso aos dados sem pagar o resgate quase impossível (pois, com a utilização de criptografia RSA 2048, a recuperação do acesso aos dados sem pagar o resgate levaria cerca de 6,4 quadriliões de anos); o *Crypto Ransomware* dimensiona cada ficheiro do sistema, determinando o valor relativo de cada um deles para o utilizador (*v.g.* fotografias, documentos do *Word* ou *Excel*, PDFs) e, de seguida, encripta os que sejam mais relevantes para o utilizador, tornando-os inutilizáveis até que o resgate seja pago; contudo, o *Crypto Ransomware* pode ir ainda mais além, existindo algumas variantes que roubam *Bitcoins* ou dados sensíveis (conversas, fotos ou outros arquivos sensíveis) à vítima que depois é ameaçada com a sua divulgação, caso não pague o resgate.

Por fim, cumpre referir que têm sido identificadas diversas famílias de *Ransomware*. De acordo com a *Symantec*, em 2015, o número de famílias de *Ransomware* identificadas era de 30, tendo sido identificadas 98 novas famílias em 2016 e 10 em 2018, após o ano de 2017 ter assistido aos terríveis ataques dos *Ransomware WannaCry* e *NotPetya* [cfr. A atividade de *ransomware* diminuiu, mas ele ainda é uma ameaça perigosa, *in https://www.symantec.com/blogs/portugues/atividade-ransomware-diminuiu-ainda-ameaca-perigosa* (acedido em 17/07/2019)].

19 Na verdade, a EUROPOL prevê que, apesar de o *Bitcoin* continuar a ser a criptomoeda mais utilizada pelos cibercriminosos, estes tendam a optar por criptomoedas que ofereçam maiores garantias de anonimato, tempos de transação mais rápidos, taxas de transação mais baixas e menos volatilidade das cotações em comparação com o *Bitcoin* ([cfr. EUROPOL, IOCTA, 2018**,** p. 63, *in www.europol.europa.eu/activities-services/main-reports/internet-organised-crimethreat-assessment-iocta -2018* (acedido em 08/06/2019)].

20 Cfr. MÁRIO ANTUNES/BALTAZAR RODRIGUES, Introdução à Cibersegurança, p. 127, JAMES A. SHERER/MELINDA L. MCLELLAN/EMILY R. FEDELES/NICHOLE L. STERLING, "Ransomware – Practical and legal considerations for confronting the new economic engine of the dark web", *in* Richmond Journal of Law & Technology, Volume XXIII, Fascículo 3, p. 30, *in https://jolt.richmond.edu/files/2017/04/Sherer-Final-May-1.pdf* (acedido em 13/06/2019), RENAN CABRAL SAISSE, **Ransomware: "sequestro" de dados e extorsão digital, in** *http://direitoeti.com.br/artigos/Ransomware-sequestro-de-dados-e-extorsao-digital/* (acedido em 11/06/2019), MASARAH PAQUET-CLOUSTON/BERNHARD HASLHOFER/BENOÎT DUPONT, "Ransomware payments in the Bitcoin ecosystem", *in* Journal of Cybersecurity, 2019, pp. 1 e ss., *in https://watermark.silverchair.com* (acedido em 13/06/2019), e EUROPOL, IOCTA, 2018**,** pp. 24 e 58, *in www.europol.europa.eu/activities-services/main-reports/internet-organised-crimethreat-assessment-iocta -2018* (acedido em 08/06/2019).

21 Que, enquanto fenómeno criminoso ou atividade criminosa também poderá ser designado como *Data jacking* (cfr. MÁRIO ANTUNES/BALTAZAR RODRIGUES, Introdução à Cibersegurança, p. 127).

informáticos[22] e a dados informáticos[23] alheios, para, numa segunda fase, bloquear os dados informáticos armazenados no sistema informático e impedir o seu titular de lhes aceder (podendo igualmente entravar esse sistema) e, numa terceira fase, exigir o pagamento de uma quantia em dinheiro para que os dados fiquem novamente acessíveis para o seu titular. Caso o resgate não seja pago, o titular ficará definitivamente privado desses dados e/ou esses dados poderão ser tornados públicos (caso tenham um conteúdo sensível) ou vendidos a terceiros (caso possuam valor comercial).

Dado que a nossa ordem jurídica não possui uma incriminação específica do *Ransomware*[24], haverá que tentar subsumir a conduta do(s) agente(s) a algum dos tipos de crime previstos na lei.

Para simplificar a exposição, iremos dividir a conduta do agente em 3 fases: (1) o acesso ilegítimo ao sistema informático e aos dados informáticos alheios, (2) o impedimento de o titular aceder aos dados e (3) a exigência e o pagamento do resgate.

---

22 Na aceção da alínea a) do artigo 2.º da Lei n.º 109/2009, de 15 de setembro.

23 Na aceção alínea b) do artigo 2.º da Lei n.º 109/2009.

24 O Código Penal da Califórnia contém uma norma que incrimina o *Ransomware* como forma de extorsão. Assim, de acordo com o §523, b) e c) desse Código:

«*b) (1) Quem, com a intenção de obter uma disposição patrimonial de outra pessoa, introduzir Ransomware em qualquer computador, sistema informático ou rede de computadores é punido, nos termos do parágrafo 520, como se tal disposição patrimonial tiver sido efetivamente obtida através de Ransomware (…)*

c) (1) "Ransomware" significa um contaminante de computador, conforme definido no parágrafo 502, ou chave colocada ou introduzida, sem autorização, num computador, sistema informático ou rede de computadores que restrinja o acesso de uma pessoa autorizada ao computador, sistema informático, rede de computadores ou a quaisquer dados neles armazenados em circunstâncias em que a pessoa responsável pela colocação ou introdução do Ransomware exija o pagamento de dinheiro ou outra disposição patrimonial para remover o contaminante do computador, restaurar o acesso ao computador, sistema informático, rede de computadores ou dados ou, de outra forma, eliminar os efeitos do contaminante ou do bloqueio do computador.

(2) O agente é responsável por colocar ou introduzir Ransomware num computador, sistema informático ou rede de computadores se colocar ou introduzir diretamente o Ransomware ou induzir outra pessoa a fazê-lo, com a intenção de exigir o pagamento de dinheiro ou outra disposição patrimonial para remover o Ransomware, restaurar o acesso ou, de outra forma, eliminar os efeitos do Ransomware».

No parágrafo 502 do mesmo Código, o legislador define "Contaminante de computador" (*Computer contaminant*) como «*qualquer conjunto de instruções de computador projetadas para modificar, danificar, destruir, registar ou transmitir informações dentro de um computador, sistema informático ou rede de computadores sem a permissão do proprietário dos dados. Elas incluem (mas não se limitam a) um grupo de instruções de computador comummente chamado vírus ou worms, que são autorreprodutoras ou autopropagáveis e são projetadas para contaminar outros programas ou dados de computador, consumir recursos do computador, modificar, destruir, gravar ou transmitir dados ou, de alguma outra forma, perturbar o normal funcionamento do computador, sistema informático ou rede de computadores*».

O legislador californiano pune a conduta de introduzir o *Ransomware* num sistema informático alheio com a intenção de obter uma disposição patrimonial (independentemente de vir a obter essa disposição patrimonial ou não) como crime de extorsão consumado. No fundo, condutas que, entre nós, seriam puníveis como crime de extorsão na forma tentada ou que nem seriam puníveis como crime de extorsão (no caso de nem chegar a ser exigido o pagamento do resgate), são punidas como crime de extorsão consumado à luz da lei californiana.

3. O IMPEDIMENTO DE O TITULAR ACEDER AOS DADOS E O (EVENTUAL) ENTRAVAMENTO DO SISTEMA INFORMÁTICO

Nesta primeira fase, o agente do crime envidará esforços para aceder ao sistema informático-alvo ou aos dados informáticos-alvo. Contudo, na maior parte das vezes, o agente não tem consigo as credenciais necessárias (por exemplo, a *password*) para aceder a esse sistema ou a esses dados e, desse modo, precisará de as obter previamente. E, para as obter, o agente do crime costuma começar por enviar à vítima ou a um seu colaborador (*v.g.* o funcionário de uma empresa, de um organismo público ou de um banco) um *e-mail* falso, simulando ter sido enviado por uma pessoa conhecida da vítima ou do seu colaborador ou por uma entidade legítima (*v.g.* uma instituição bancária, uma entidade policial, etc.)[25], convidando-o(a) a baixar um dado ficheiro, abrir um anexo, clicar e abrir um *link*, etc. (incluindo campanhas massivas de *Spear Phishing*[26], utilizando o método "*spray and*

25 Cfr. JAMES A. SHERER/MELINDA L. MCLELLAN/EMILY R. FEDELES/NICHOLE L. STERLING, "Ransomware – Practical and legal considerations for confronting the new economic engine of the dark web", *in* Richmond Journal of Law & Technology, Volume XXIII, Fascículo 3, pp. 10-11, *in* *https://jolt.richmond.edu/files/2017/04/Sherer-Final-May-1.pdf* (acedido em 13/06/2019).

No caso do *WannaCry*, o *malware* foi disseminado através de um *e-mail* contendo um ficheiro ZIP anexo, que, sendo aberto, infetava o sistema informático [cfr. ELIŠKA NOVÁČKOVÁ, Current Cyberthreats and Relevant Legal Instruments *in* EU and Canada, p. 6 *in* *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3215960* (acedido em 11/07/2019)].

Contudo, a obtenção ilegítima das credenciais poderá ocorrer de qualquer outra forma, como, por exemplo, o agente do crime ver um seu colega de trabalho digitar a *password* ou este, por qualquer razão, lhe facultar essa mesma *password*. Também é possível que o acesso seja conseguido sem qualquer "interação" humana, pois existem versões de *Ransomware* que procuram sistemas vulneráveis através de um massivo *scanning* de sistemas informáticos executado remota e sub-repticiamente [cfr. TERRENCE AUGUST/DUY DAO/MARIUS FLORIN NICULESCU, Economics of Ransomware Attacks, p. 1, *in* *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3351416* (acedido em 13/06/2019)].

26 O *Phishing* consiste na obtenção *online*, de forma fraudulenta, de dados pessoais (*v.g.* credenciais de acesso a contas bancárias) para ulterior utilização maliciosa (*v.g.* efetuar movimentos nas contas bancárias da vítima, aquisições de bens ou transferências para contas pertencentes ao agente do crime). Em regra, o *Phishing* inicia-se com o envio de um *e-mail*, aparentemente de uma fonte confiável, que encaminha o alvo para um *site* falso onde está o *malware* ou contém um ficheiro ou *link* que, sendo aberto, instala o *malware* no sistema informático, dando acesso a esse sistema e aos dados nele armazenados para ulterior utilização maliciosa.

Por seu turno, o *Spear Phishing* é uma forma de *Phishing* que se caracteriza por consistir num ciberataque que atinge um ou mais alvos específicos e determinados, em vez de ataques amplos e dispersos. Encontramos um exemplo de *Spear Phishing* no caso de um grupo criminoso, que, entre 2013 e 2017, fazendo uso dos programas de *malware* Carbanak e Cobalt, atacou mais de 100 instituições bancárias, sistemas de pagamento e outras instituições financeiras em mais de 40 países, resultando em perdas acumuladas de mais de mil milhões de euros no setor financeiro. Para acederem à rede bancária interna das instituições bancárias atingidas e infetarem os servidores que controlavam as caixas eletrónicas, os criminosos começavam por enviar aos funcionários de cada um dos bancos *e-mails* que aparentavam provir de empresas legítimas e cujos anexos continham *malware*. Uma vez descarregado, o *software* malicioso permitia que os criminosos controlassem remotamente as máquinas infetadas, conseguindo aceder à rede bancária interna e aos servidores que controlavam as caixas eletrónicas [cfr. EUROPOL, Carbanak/Cobalt Infographic, *in* *https://www.europol.europa.eu/publications-documents/carbanak/cobalt-infographic* (acedido em 04/07/2018)].

pray"[27])[28], o que, sendo feito, permite a instalação *sub-reptícia* de um *malware* que dará ao agente o acesso ao sistema ou aos dados. Outra forma de disseminação de *Ransomware* é através da disponibilização de *software* infetado para *download* gratuito na Internet[29]. Porém, este procedimento "preliminar" poderá não ser necessário, pois o agente do crime pode possuir, legitimamente, as credenciais necessárias que depois utilizará para executar o crime[30].

O envio de *e-mail* falso simulando ter sido enviado por uma pessoa conhecida da vítima ou por uma entidade legítima com a finalidade de, por ação de quem recebe o *e-mail*, ser instalado um *malware* que permitirá ao agente aceder ao sistema ou aos dados-alvo, configura a prática de um crime de falsidade informática, p. e p. pelo artigo 3.º da Lei n.º 109/2009. Do mesmo modo, a inserção, pelo agente, das credenciais de outra pessoa (*v.g.* de um seu colega de trabalho) num sistema informático para aceder ao sistema ou aos dados-alvo também configura a prática de um crime de falsidade informática, p. e p. pelo artigo 3.º da Lei n.º 109/2009, nos termos do qual:

---

27 O método "*spray* and *pray*" consiste em disponibilizar ficheiros infetados para *download*, enviar (em regra massivamente) *e-mails* infetados, etc., esperando que alguém, desconhecendo que estão infetados e não possuindo um sistema informático suficientemente protegido, baixe os ficheiros infetados ou os destinatários dos *e-mails* atuem de acordo com o sugerido nesses *e-mails* (baixando um dado ficheiro, abrindo um anexo, clicando e abrindo um *link*, etc.) [cfr. JAMES A. SHERER/MELINDA L. MCLELLAN/EMILY R. FEDELES/NICHOLE L. STERLING, "Ransomware – Practical and legal considerations for confronting the new economic engine of the dark web", *in* Richmond Journal of Law & Technology, Volume XXIII, Fascículo 3, p. 12, *in* *https://jolt.richmond.edu/files/2017/04/Sherer-Final-May-1.pdf* (acedido em 13/06/2019)].

28 Cfr. JAMES A. SHERER/MELINDA L. MCLELLAN/EMILY R. FEDELES/NICHOLE L. STERLING, "Ransomware – Practical and legal considerations for confronting the new economic engine of the dark web", *in* Richmond Journal of Law & Technology, Volume XXIII, Fascículo 3, pp. 10-11, *in* *https://jolt.richmond.edu/files/2017/04/Sherer-Final-May-1.pdf* (acedido em 13/06/2019).

29 Cfr. JAMES A. SHERER/MELINDA L. MCLELLAN/EMILY R. FEDELES/NICHOLE L. STERLING, "Ransomware – Practical and legal considerations for confronting the new economic engine of the dark web", *in* Richmond Journal of Law & Technology, Volume XXIII, Fascículo 3, p. 10, *in* *https://jolt.richmond.edu/files/2017/04/Sherer-Final-May-1.pdf* (acedido em 13/06/2019).

30 No fundo, haverá que destrinçar, nesta primeira fase, os casos em que o agente possui, legitimamente, as credenciais de acesso dos casos em que não as possui *ab initio* e irá obtê-las. E, em regra, essa obtenção será levada a cabo mediante a indução da vítima ou de um terceiro em erro (*v.g.* enviando-lhe um *e-mail* falso nos termos referidos no texto.

Contudo, embora o Cibercrime tenha um cariz essencialmente sub-reptício, não será de excluir a possibilidade de, em casos muito excecionais, o agente obter as credenciais de acesso mediante o recurso à violência e/ou a ameaças (do uso de violência, de revelação de factos "incómodos", etc.), caso em que estaremos perante a prática de um crime de coação (p. e p. pelo artigo 154.º do Código Penal) ou mesmo de um crime de coação agravada (p. e p. pelo artigo 155.º do Código Penal) em concurso efetivo com o crime de ofensa à integridade física, no caso de a coação for levada a cabo mediante agressões a outra pessoa qualificáveis como ofensa à integridade física grave nos termos do artigo 144.º do Código Penal (cfr. TAIPA DE CARVALHO, "Artigo 154º", *in* Comentário Conimbricense do Código Penal, I, 2.ª Edição, p. 584, considerando que a pena estabelecida para o crime de coação já considera o mínimo de violência - que consubstancia uma ofensa à integridade física simples - que a coação pressupõe; diversamente, PINTO DE ALBUQUERQUE, Comentário do Código Penal, p. 418, defende a existência de concurso efetivo entre os crimes de coação e de ofensa à integridade física sem estabelecer qualquer destrinça entre ofensa simples e grave).

«*1 – Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias.*

2 – Quando as ações descritas no número anterior incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, a pena é de 1 a 5 anos de prisão.

3 – Quem, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar documento produzido a partir de dados informáticos que foram objeto dos atos referidos no n.º 1 ou cartão ou outro dispositivo no qual se encontrem registados ou incorporados os dados objeto dos atos referidos no número anterior, é punido com as penas previstas num e noutro número, respetivamente.

4 – Quem importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das ações prevista no n.º 2, é punido com pena de prisão de 1 a 5 anos.

6 – Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de 2 a 5 anos.».

A essência do crime de falsidade informática reside na manipulação dos dados inseridos num sistema informático ou do seu tratamento, de que resultará a criação de documentos ou dados falsos, lesando a segurança e a fiabilidade dos documentos no tráfico jurídico-probatório[31]; esta incriminação visa equiparar, no plano do Direito penal, a adulteração de documentos eletrónicos à adulteração de documentos na aceção da alínea a) do artigo 255.º do

31 Cfr. FARIA COSTA, "Algumas reflexões sobre o estatuto dogmático do chamado "Direito penal informático"", *in* Direito Penal da Comunicação, p. 109, e DUARTE RODRIGUES NUNES, O crime de falsidade informática, *in http://julgar.pt/o-crime-de-falsidade-informatica/* (acedido em 19/07/2019).

Discute-se, na Doutrina e na Jurisprudência, qual é o bem jurídico tutelado pelo crime de falsidade informática, encontrando-se três correntes: uma primeira, que considera que é a integridade dos sistemas informáticos; uma segunda, que entende que é a segurança nas transações bancárias; e uma terceira (que subscrevemos), que considera que é a segurança e a fiabilidade dos documentos no tráfico jurídico-probatório (*i.e.*, o mesmo bem jurídico tutelado pelo crime de falsificação p. e p. pelo artigo 256.º do Código Penal). No entanto, uma abordagem mais detida desta questão não se justifica no âmbito do presente estudo.

Código Penal no âmbito do crime de falsificação de documento, p. e p. pelo artigo 256.º do Código Penal[32].

Assim, ao criar e enviar o *e-mail* falso, o agente do crime está a introduzir dados informáticos (falsos) no sistema informático em que tal *e-mail* é criado[33] e enviado, produzindo (e enviando) um *e-mail* falso, com a intenção de que seja considerado genuíno pelo destinatário, que, crendo na sua genuinidade, adotará a conduta "solicitada" nesse *e-mail* (*v.g.* baixar um ficheiro, abrir um anexo, clicar e abrir um *link*, etc.), permitindo que o agente, posteriormente, aceda ao sistema informático-alvo ou aos dados nele armazenados ou acessíveis através dele (*v.g.* dados armazenados numa nuvem que possam ser acedidos através do sistema informático em causa). E, ao inserir as credenciais de acesso de um terceiro, o agente está a introduzir dados falsos[34] num sistema informático, que, "crendo" tratar-se do legítimo detentor das credenciais de acesso, permite-lhe aceder ao sistema ou aos dados nele armazenados ou acessíveis através dele.

Nesta situação, o crime de falsidade informática surge como uma espécie de ato preparatório do crime de acesso ilegítimo. Mas o agente será sempre punido pelo crime de falsidade informática, pois, além de o crime de falsidade informática ser punido com uma pena mais elevada do que o crime de acesso ilegítimo[35], os bens jurídicos tutelados por ambas as incriminações (a segurança do sistema informático no crime de acesso ilegítimo[36] e a segurança

32 Cfr. PEDRO VERDELHO, "Lei n.º 109/2009, de 15 de Setembro", *in* Comentário das Leis Penais Extravagantes, I, pp. 505-506, e DUARTE RODRIGUES NUNES, O crime de falsidade informática, *in http://julgar.pt/o-crime-de-falsidade-informatica/* (acedido em 19/07/2019).

33 Tutelando o crime de falsidade informática a segurança e a fiabilidade dos documentos no tráfico jurídico-probatório, a manipulação de dados próprios do agente (ou do seu tratamento automático) inseridos num sistema informático igualmente do próprio agente (*v.g.* quando um comerciante altera um programa informático para obter um resultado que vicia a sua própria escrituração) configura a prática do crime de falsidade informática, uma vez que, nesse caso, continuará a estar em causa a proteção da segurança e da fiabilidade dos documentos no tráfico jurídico-probatório, que também são lesadas quando o agente manipula dados informáticos que lhe pertencem (ou manipula o seu tratamento automático) e que estejam inseridos num sistema informático que igualmente lhe pertence [cfr. OLIVEIRA ASCENSÃO, "Criminalidade informática", *in* Direito da Sociedade da Informação, II, p. 222, e DUARTE RODRIGUES NUNES, O crime de falsidade informática, *in http://julgar.pt/o-crime-de-falsidade-informatica/* (acedido em 19/07/2019)].

34 Ainda que os dados inseridos sejam legítimos, são inseridos por uma pessoa diversa do legítimo detentor das credenciais de acesso, levando o sistema a assumir erradamente que se trata da pessoa que detém legitimamente essas credenciais e a permitir o acesso.

35 A pena do crime de falsidade informática poderá chegar, mesmo na sua forma simples, a 5 anos de prisão, ao passo que o crime de acesso ilegítimo, só nos casos subsumíveis ao n.º 4 do artigo 6.º da Lei n.º 109/2009 é que a pena poderá atingir os 5 anos, não indo além de 1 ano nos casos subsumíveis ao n.º 1 e de 3 anos nos casos subsumíveis ao n.º 3 desse preceito. Daí que, caso se considerasse que existia um concurso aparente de crimes, sempre conduziria a uma situação de consunção impura, que, como sabemos, consiste em, nos casos em que o crime "dominado" seja punível com uma pena mais grave do que o crime "dominante", o agente ser punido por aquele crime e não por este (cfr. FIGUEIREDO DIAS, Direito Penal, Parte Geral, I, 2.ª Edição, p. 1023).

36 Cfr. LOURENÇO MARTINS, "Criminalidade informática", *in* Direito da Sociedade da Informação, IV, p. 29, e DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime (em publicação).

e a fiabilidade dos documentos no tráfico jurídico-probatório no crime de falsidade informática) são diversos, existindo, por isso, concurso efetivo[37].

Quanto ao acesso propriamente dito, a conduta de aceder a um dado sistema informático ou aos dados nele armazenados ou acessíveis através dele (v.g. dados armazenados numa nuvem que possam ser acedidos através do sistema informático em causa) constitui um crime de acesso ilegítimo, p. e p. pelo artigo 6.º da Lei n.º 109/2009, nos termos do qual:

«*1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.*

2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as ações não autorizadas descritas no número anterior.

3 - A pena é de prisão até 3 anos ou multa se o acesso for conseguido através de violação de regras de segurança.

4 - A pena é de prisão de 1 a 5 anos quando:

a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou

b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.

5 - A tentativa é punível, salvo nos casos previstos no n.º 2.

5- *Nos casos previstos nos n.ºs 1, 3 e 5 o procedimento penal depende de queixa*.».

A essência do crime de acesso ilegítimo assenta em o agente do crime aceder a um sistema informático alheio sem autorização legal ou do respetivo titular ou, existindo uma tal

---

É discutido, na Doutrina e na Jurisprudência, qual é o bem jurídico tutelado pelo crime de acesso ilegítimo, encontrando-se três correntes: uma primeira, que considera que é o património do lesado e a segurança dos sistemas informáticos e, nos casos previstos no n.º 4 do artigo 6.º da Lei n.º 109/2009, a concorrência e a liberdade de comércio e, quando estejam em causa valores elevados, a segurança jurídica; uma segunda, que entende que é a privacidade, funcionando a proteção da segurança e da privacidade do sistema informático como uma mera decorrência da proteção da privacidade; e uma terceira (que subscrevemos), que considera que é apenas a segurança do sistema informático (estando em causa salvaguardar a possibilidade de gerir, operar e controlar os sistemas de forma livre e tranquila, sem perturbação). Também aqui não se justifica uma abordagem mais detida no âmbito do presente estudo.

37 Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime (em publicação).

autorização, violando os limites da mesma[38]. Estamos perante uma conduta que, além de constituir crime *ex se*, facilita o cometimento de outros crimes (*v.g.* os crimes de dano relativo a programas ou outros dados informáticos, de sabotagem informática, de interceção ilegítima ou de burla informática e nas comunicações), podendo a criminalização do acesso ilegítimo ser vista como uma proteção antecipada e indireta contra os danos que afetem dados informáticos e a espionagem informática[39].

Assim, ao aceder ao sistema informático e aos dados nele armazenados ou acessíveis através dele sem autorização legal ou do proprietário ou de outro titular do direito do sistema ou de parte dele[40], o agente adota uma conduta subsumível ao n.º 1 do artigo 6.º da Lei n.º 109/2009. Contudo, o acesso ilegítimo ocorrerá com a utilização de credenciais de acesso ou de mecanismos destinados a neutralizar a proteção proporcionada pela exigência da "apresentação" das credenciais mediante, por exemplo, a inserção de uma *password* e, desse modo, será conseguido através da violação de regras de segurança[41], pelo que a conduta é subsumível ao n.º 3 do artigo 6.º da Lei n.º 109/2009.

---

38 Cfr. PEDRO VERDELHO, "Lei n.º 109/2009, de 15 de Setembro", *in* Comentário das Leis Penais Extravagantes, I, p. 516, e Acórdãos da Relação de Lisboa de 11/04/2018, da Relação do Porto de 08/01/2014 e da Relação de Coimbra de 17/02/2016, *in www.dgsi.pt.*

De acordo com PEDRO VERDELHO, *Op. e Loc. Cit.*, «*o crime de acesso ilegítimo dirige-se às modernas ameaças à segurança dos sistemas informáticos que ponham em causa as respectivas confidencialidade, integridade e disponibilidade*».

39 Cfr. LOPES ROCHA, "A lei da criminalidade informática (Lei n.º 109/01 de 17 de Agosto). Génese e técnica legislativa", *in* Cadernos de Ciência de Legislação, n.º 8, p. 75.

40 A autorização do proprietário ou de outro titular do direito do sistema ou de parte dele constitui uma situação de acordo que exclui a tipicidade e que se distingue do consentimento enquanto causa de justificação pelo facto de, no acordo, estar em causa o exercício do direito de liberdade pela pessoa que o concede, correndo a realização da conduta no mesmo sentido da tutela do bem jurídico, não se podendo falar, por essa razão, de uma lesão do bem jurídico; diversamente, no caso do consentimento, ocorre uma lesão efetiva do bem jurídico, cuja ilicitude é afastada por via da colisão entre o interesse jurídico-penal na preservação de bens jurídicos com o interesse, igualmente com relevo jurídico-penal, na salvaguarda da autorrealização do titular do bem jurídico (que terá de ser disponível), da sua autonomia pessoal e da sua vontade. Acerca da distinção entre consentimento e acordo (que exclui a tipicidade), *vide* COSTA ANDRADE, Consentimento e Acordo em Direito Penal, pp. 257 e ss. e 506 e ss, e FIGUEIREDO DIAS, Direito Penal, Parte Geral, I, 2.ª Edição, pp. 472 e ss.

41 Cfr. PEDRO VERDELHO, "Lei n.º 109/2009, de 15 de Setembro", *in* Comentário das Leis Penais Extravagantes, I, p. 516, e ROGÉRIO BRAVO, O Crime de Acesso Ilegítimo na Lei da Criminalidade Informática e na CiberConvenção, *in http://www.academia.edu* (acedido em 18/07/2018).

Como refere ROGÉRIO BRAVO, *Op. Cit.*, a violação de regras de segurança consiste em «*qualquer acto suportado por tecnologias de informação e de comunicação, que constitua a transformação, a simulação, a decifração, a neutralização temporária ou a anulação, de meios técnicos destinados a assegurar a autenticação de serviços resultantes da acção de programas informáticos e de utilizadores legítimos, bem como a procura activa de elementos que possam permitir o acesso perante um sistema ou uma rede informática ou de comunicações*». Assim, a violação de regras de segurança poderá consistir em o acesso ocorrer mediante a utilização de um PIN, *password* ou outro código de acesso ilegitimamente obtido pelo agente (o que inclui os tradicionais meios de autenticação simétrica e os meios de autenticação assentes no recurso a técnicas biométricas, bem como outros que venham a ser disponibilizados pelo progresso tecnológico).

Mas, atenta a fenomenologia do *Ransomware*, não será de excluir a subsunção da conduta a alguma das circunstâncias modificativas agravantes do n.º 4 do artigo 6.º da Lei n.º 109/2009[42]. Assim, desde logo nos casos em que a conduta criminosa seja dirigida contra um banco, uma empresa ou um organismo público, é altamente provável que, ao aceder ao sistema e aos dados, o agente acabe por tomar conhecimento de segredo comercial ou industrial[43] ou de dados confidenciais protegidos por lei (que serão as informações mais "valiosas" para efeitos de exigência do pagamento de um resgate pela "restituição" do acesso aos dados).

Cumpre ainda referir que o agente, mesmo nos casos em que possua, de forma legítima, as credenciais de acesso, comete o crime de acesso ilegítimo, pois, como referimos, o crime de acesso ilegítimo inclui também os casos em que o agente atua ao abrigo de uma autorização legal ou do proprietário ou de outro titular do direito do sistema ou de parte dele, mas viola os limites da mesma.

A este respeito, a Relação do Porto, no seu Acórdão de 14/04/2004[44], considerou que o agente cometeu um crime de acesso ilegítimo num caso em que, quando cessou a relação laboral entre o agente e a assistente, aquele retirou do sistema informático desta o código-fonte de um programa que desenvolvera enquanto fora seu trabalhador.

Do mesmo modo, a Relação de Lisboa, nos seus Acórdãos de 25/11/2015 e 11/04/2018[45], considerou que o agente cometeu um crime de acesso ilegítimo num caso em que, sendo trabalhador do assistente e dispondo de uma chave de acesso única, pessoal e intransmissível (que lhe permitia aceder ao sistema informático do assistente e visualizar os elementos deste constantes, bem como realizar e autorizar operações bancárias através do mesmo), sem qualquer motivo ou razão de serviço que o justificasse (e extravasando a autorização de acesso que o assistente lhe conferira), acedeu ao sistema informático do assistente utilizando a sua *password* para proceder à consulta de várias contas de depósito de

42 Que, afastarão a aplicabilidade do n.º 3 desse preceito, que funcionará apenas como circunstância a valorar ao nível da determinação da medida concreta da pena, mais concretamente como circunstância agravante [cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime (em publicação)].

43 Seguindo de perto o disposto nos arts. 313.º a 315.º do Código da Propriedade Industrial, estão em causa informações relativas à vida e organização de uma empresa que não são geralmente conhecidas ou facilmente acessíveis (na sua globalidade ou na configuração e ligação exatas dos seus elementos constitutivos) a pessoas dos círculos que lidam normalmente com o tipo de informações em questão, que tenham valor comercial por serem secretas e que tenham sido objeto de diligências consideráveis, atendendo às circunstâncias, por parte da pessoa que detém legalmente o controlo das informações, no sentido de as manter secretas. Caberão aqui, por exemplo, informações relativas ao fabrico ou comercialização de produtos ou à prestação de serviços, à organização administrativa ou financeira da empresa, às relações entre a empresa e os seus fornecedores ou entre a empresa e os seus clientes, etc., que concedam uma vantagem competitiva no mercado a quem possuir tais informações.

44 *In www.dgsi.pt*.

45 *In www.dgsi.pt*.

clientes e realizar transferências de dinheiro. E a mesma Relação, no seu Acórdão de 07/03/2018[46], chegou à mesma conclusão num caso em que os agentes, extravasando as suas competências funcionais, acederam a dados de tráfego de um jornalista junto de uma operadora de telecomunicações para fins exclusivamente pessoais.

Por seu turno, a Relação de Coimbra, no seu Acórdão de 17/02/2016[47], considerou que o agente cometeu um crime de acesso ilegítimo num caso em que, sendo inspetor tributário e, não obstante deter legitimamente, para o exercício das suas funções, *username* e PIN, por motivos estritamente pessoais, acedeu ao sistema informático da Autoridade Tributária para consultar declarações de IRS de outra pessoa.

Como referimos, não é de excluir a possibilidade (embora tendencialmente rara) de as credenciais de acesso serem obtidas mediante o recurso à violência e/ou a ameaças, caso em que estaremos perante a prática de um crime de coação simples (p. e p. pelo artigo 154.º do Código Penal) ou agravada (p. e p. pelo artigo 155.º do Código Penal) em concurso – se for o caso – com um crime de ofensa à integridade física grave (p. e p. pelo artigo 144.º do Código Penal), pois tutelam bens jurídicos diversos[48]. Deste modo, tutelando o crime de coação e o crime de ofensa à integridade física qualificada bens jurídicos diversos e igualmente diversos dos bens jurídicos tutelados pelos crimes de falsidade informática e de acesso ilegítimo, existirá uma situação de concurso efetivo entre todos estes crimes sempre que o agente pratique factos subsumíveis a cada um deles.

46 *In www.dgsi.pt.*
47 *In www.dgsi.pt.*
48 O crime de coação (simples ou agravada) tutela a liberdade de decisão e de ação (cfr. TAIPA DE CARVALHO, "Artigo 154º", *in* Comentário Conimbricense do Código Penal, I, 2.ª Edição, p. 569, e PINTO DE ALBUQUERQUE, Comentário do Código Penal, p. 415), ao passo que o crime de ofensa à integridade física qualificada tutela a integridade física (cfr. PAULA RIBEIRO DE FARIA, "Artigo 144º", *in* Comentário Conimbricense do Código Penal, I, 2.ª Edição, p. 339, e PINTO DE ALBUQUERQUE, *Op. Cit.*, p. 388), sendo que não se pode considerar as ofensas previstas no artigo 144.º do Código Penal como tidas em conta na pena estabelecida para o crime de coação, pois não estamos perante uma situação qualificável como "um mínimo de violência" (cfr. TAIPA DE CARVALHO, *Op. Cit.*, p. 584).

4. A EXIGÊNCIA E O PAGAMENTO DO RESGATE

Conseguido o acesso ao sistema informático e aos dados nele armazenados ou acessíveis através dele, a etapa seguinte será impedir o legítimo titular de aceder aos dados. Para isso, os dados irão ser, sub-repticiamente, criptografados, compactados com senhas ou – embora menos frequentemente - apagados (mas guardados pelo agente)[49], assim se impedindo o legítimo titular de lhes aceder[50]. Tal conduta configura a prática de um crime de dano relativo a programas ou outros dados informáticos, p. e p. pelo artigo 4.º da Lei n.º 109/2009, nos termos do qual:

«*1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afetar a capacidade de uso, é punido com pena de prisão até 3 anos ou pena de multa.*

2 - A tentativa é punível.

3 - Incorre na mesma pena do n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as ações não autorizadas descritas nesse número.

4 - Se o dano causado for de valor elevado, a pena é de prisão até 5 anos ou de multa até 600 dias.

5 - Se o dano causado for de valor consideravelmente elevado, a pena é de prisão de 1 a 10 anos.

---

49 Cfr. JAMES A. SHERER/MELINDA L. MCLELLAN/EMILY R. FEDELES/NICHOLE L. STERLING, "Ransomware – Practical and legal considerations for confronting the new economic engine of the dark web", *in* Richmond Journal of Law & Technology, Volume XXIII, Fascículo 3, p. 14, *in* *https://jolt.richmond.edu/files/2017/04/Sherer-Final-May-1.pdf* (acedido em 13/06/2019).

50 Cfr. RENAN CABRAL SAISSE, **Ransomware: "sequestro" de dados e extorsão digital, in** *http://direitoeti.com.br/artigos/Ransomware-sequestro-de-dados-e-extorsao-digital/* (acedido em 11/06/2019).

De acordo com JAMES A. SHERER/MELINDA L. MCLELLAN/EMILY R. FEDELES/NICHOLE L. STERLING, "Ransomware – Practical and legal considerations for confronting the new economic engine of the dark web", *in* Richmond Journal of Law & Technology, Volume XXIII, Fascículo 3, p. 14, *in* *https://jolt.richmond.edu/files/2017/04/Sherer-Final-May-1.pdf* (acedido em 13/06/2019), existem versões de *Ransomware* que rastreiam o sistema informático para detetarem quais são os dados "sensíveis" cuja encriptação para posterior exigência de pagamento de resgate se "justifica".

6 - Nos casos previstos nos n.ºs 1, 2 e 4 o procedimento penal depende de queixa».

A essência do crime de dano relativo a programas ou outros dados informáticos reside na supressão, inutilização ou danificação de dados informáticos, visando-se conferir aos dados informáticos (enquanto bens incorpóreos), no plano do Direito penal, uma proteção análoga à tutela dos bens corpóreos através do crime de dano p. e p. pelos arts. 212.º e ss. do Código Penal[51].

A conduta de bloquear o acesso aos dados, tornando-os inacessíveis até que seja pago o resgate, configura uma supressão de dados informáticos[52], sendo subsumível ao n.º 1 do artigo 4.º da Lei n.º 109/2009, pois o agente atua sem permissão legal ou autorização do proprietário ou de outro titular do direito do sistema ou de parte dele.

Tutelando o crime de dano relativo a programas ou outros dados informáticos a integridade dos dados e o bom funcionamento dos programas[53], existirá sempre uma situação de concurso efetivo com os tipos de crime que referimos que poderão estar em causa na fase do acesso (ilegítimo) ao sistema e aos dados, à exceção do crime de falsidade informática, em que a solução terá de ser casuística (existindo, nuns casos, concurso efetivo e, noutros, concurso aparente)[54].

---

51 Cfr. PEDRO VERDELHO, "Cibercrime", *in* Direito da Sociedade da Informação, IV, p. 365, e DUARTE RODRIGUES NUNES, "O crime de dano relativo a programas ou outros dados informáticos", *in* Revista do Ministério Público, n.º 153, p. 141.

52 O ato de "suprimir" consiste «*na retenção, ocultação, em tornar temporariamente indisponíveis dados que se encontrem num sistema informático*» (cfr. DUARTE RODRIGUES NUNES, "O crime de dano relativo a programas ou outros dados informáticos", *in* Revista do Ministério Público, n.º 153, p. 148).

Todavia, nos casos em que, como referem JAMES A. SHERER/MELINDA L. MCLELLAN/EMILY R. FEDELES/NICHOLE L. STERLING, "Ransomware – Practical and legal considerations for confronting the new economic engine of the dark web", *in* Richmond Journal of Law & Technology, Volume XXIII, Fascículo 3, p. 14, *in* *https://jolt.richmond.edu/files/2017/04/Sherer-Final-May-1.pdf* (acedido em 13/06/2019), os agentes do crime apagam os dados, estaremos perante uma destruição/apagamento dos dados informáticos.

53 Cfr. GARCIA MARQUES/LOURENÇO MARTINS, Direito da Informática, 2.ª Edição, pp. 690-691, BENJAMIM SILVA RODRIGUES, Da Prova Penal, IV, pp. 139-140, e DUARTE RODRIGUES NUNES, "O crime de dano relativo a programas ou outros dados informáticos", *in* Revista do Ministério Público, n.º 153, pp. 144-145.

Discute-se, na Doutrina e na Jurisprudência, qual é o bem jurídico tutelado pelo crime de dano relativo a programas ou outros dados informáticos, encontrando-se duas correntes: uma primeira, que considera que é a integridade dos dados e o bom funcionamento dos programas (que subscrevemos); e uma segunda, que entende que é património. No entanto, não se justifica no âmbito do presente estudo uma abordagem mais detida desta questão.

54 Por um lado, ambas as incriminações tutelam bens jurídicos diversos, mas, por outro, as condutas de modificação (que é similar a alteração), apagamento ou supressão de dados informáticos são comuns a ambos os tipos de crime.

Assim, quando o agente atue com as finalidades referidas no n.º 1 do artigo 3.º da Lei n.º 109/2009 e da manipulação resulte a produção de dados ou documentos não genuínos, mas, ao mesmo tempo, acabe por, pelo menos com dolo eventual, afetar o funcionamento dos dados informáticos, bem como nos casos em que a conduta consista na modificação (que é similar a alteração), apagamento ou supressão de dados informáticos para as finalidades referidas no n.º 1 do artigo 3.º da Lei n.º 109/2009, mas inclua igualmente alguma das demais condutas

De notar, por último, que, dado que as principais vítimas do *Ransomware* costumam ser empresas (sobretudo empresas já com uma certa dimensão), bancos e organismos públicos, tenderá a ser mais frequente o cometimento do crime de dano relativo a programas ou outros dados informáticos na sua forma qualificada (nos termos do n.º 4 ou do n.º 5 do artigo 4.º da Lei n.º 109/2009[55]) do que na sua forma simples.

O bloqueio do acesso aos dados mediante a sua supressão (ou destruição/apagamento) também poderá entravar, impedir, interromper ou perturbar gravemente o funcionamento do sistema informático em causa[56], o que configura a prática de um crime de sabotagem informática, p. e p. pelo artigo 5.º da Lei n.º 109/2009, nos termos do qual:

«*1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias.*

previstas no n.º 1 do artigo 4.º, tutelando ambas as incriminações bens jurídicos diversos, existirá uma relação de concurso efetivo.

Nos demais casos, dado que as condutas de modificação (que é similar a alteração), apagamento ou supressão de dados informáticos estão abrangidas por ambas as incriminações, existirá concurso aparente, sendo que, nos casos em que o agente atue com as finalidades referidas no n.º 1 do artigo 3.º da Lei n.º 109/2009 e da manipulação resulte a produção de dados ou documentos não genuínos, será punido pelo crime de falsidade informática, sendo punido pelo crime de dano relativo a programas ou outros dados informáticos nos demais casos [cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime (em publicação)].

55 Os prejuízos causados com a supressão dos dados informáticos (que nada têm a ver com o eventual pagamento do resgate) tenderão a ser de valor elevado ou consideravelmente elevado, atento os conceitos constantes das alíneas a) e b) do artigo 202.º do Código Penal.

56 Cfr. RENAN CABRAL SAISSE, **Ransomware: "sequestro" de dados e extorsão digital, in** *http://direitoeti.com.br/artigos/Ransomware-sequestro-de-dados-e-extorsao-digital/* (acedido em 11/06/2019).

"Entravar" consiste na incapacitação definitiva e total, na destruição integral do sistema informático (não sendo, contudo, necessária a sua destruição física, bastando que esse sistema informático deixe, em definitivo, de funcionar). "Impedir" consiste na incapacitação definitiva, mas não total do sistema informático, permitindo apenas o seu funcionamento parcial. "Interromper" consiste na incapacitação apenas temporária do sistema informático, que, de forma meramente temporária, deixará de funcionar, no todo ou em parte. E, por último, "perturbar gravemente" consiste nas situações, em que, apesar de o sistema não deixar de funcionar, o funcionamento ocorre com perturbações, interferências (*v.g.* de forma mais lenta ou obrigando a *restarts* do sistema), devendo essas perturbações ou interferências possuir algum relevo ou alguma gravidade, pelo que, por exemplo, a maior lentidão terá de ser significativa e não apenas ligeira [cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime (em publicação)].

Contudo, sendo o crime de sabotagem informática punido apenas a título de dolo (sendo suficiente o dolo eventual), o agente, ao suprimir os dados, terá de ter agido, pelo menos com dolo eventual, quanto ao entravamento do sistema informático por via dessa supressão, caso contrário, será punido apenas pelo crime de dano relativo a programas ou outros dados informáticos.

2 – Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as ações não autorizadas descritas no número anterior.

3 – Nos casos previstos no número anterior, a tentativa não é punível.

4 – A pena é de prisão de 1 a 5 anos se o dano emergente da perturbação for de valor elevado.

5 – A pena é de prisão de 1 a 10 anos se:

a) O dano emergente da perturbação for de valor consideravelmente elevado;

b) A perturbação causada atingir de forma grave ou duradoura um sistema informático que apoie uma atividade destinada a assegurar funções sociais críticas, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos.».

A essência do crime de sabotagem informática reside na «*destruição, inutilização ou paralisação dos sistemas informáticos e telemáticos, ou de dados ou informação contida, transferida ou transmitida nos mesmos, assim como das suas funções de processamento e tratamento, seja mediante a utilização de métodos lógicos, informáticos ou telemáticos, seja mediante o abuso de equipamentos físicos*»[57].

Tal como referimos quanto ao crime de dano relativo a programas ou outros dados informáticos e pelas mesmas razões, também no caso do crime de sabotagem informática tenderá a ser mais frequente o cometimento do crime na sua forma qualificada (nos termos do n.º 4 ou do n.º 5 do artigo 5.º da Lei n.º 109/2009[58]) do que na sua forma simples (cfr. n.º 1 do artigo 5.º), pois o prejuízo causado será tendencialmente de valor elevado ou mesmo consideravelmente elevado. Mas, no caso da sabotagem informática a conduta do agente também poderá ser subsumível a uma outra circunstância modificativa agravante, que não

57 BENJAMIM SILVA RODRIGUES, Da Prova Penal, IV, p. 149. LOURENÇO MARTINS, "Criminalidade informática", *in* Direito da Sociedade da Informação, IV, pp. 25-26, considera que a sabotagem informática constitui uma conduta mais grave do que o dano relativo a programas ou outros dados informáticos, por entravar ou perturbar o funcionamento do próprio sistema informático (e não apenas a destruição dos dados), bastando pensar no facto de o sistema informático ser utilizado para fins militares, de apoio médico, de regulação do trânsito ou de exercício da atividade bancária ou seguradora.

58 Os prejuízos causados com a supressão dos dados informáticos (que nada têm a ver com o eventual pagamento do resgate) tenderão a ser de valor elevado ou consideravelmente elevado, atento os conceitos constantes das alíneas a) e b) do artigo 202.º do Código Penal.

existe no crime de dano relativo a programas ou outros dados informáticos: a perturbação causada atingir de forma grave ou duradoura[59] um sistema informático que apoie uma atividade destinada a assegurar funções sociais críticas[60], nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos. E, tendo em conta os alvos habituais do *Ransomware*, cremos que não será arriscado afirmar que, nos casos em que o agente tenha cometido igualmente o crime de sabotagem informática, a subsunção da conduta a esta circunstância modificativa agravante tenderá a ser frequente.

De todo o modo, quando o agente tenha agido com, no mínimo, dolo eventual quanto ao entravamento do sistema, existirá uma relação de concurso efetivo entre os crimes de sabotagem informática (que tutela a integridade e o bom funcionamento dos sistemas informáticos e das comunicações eletrónicas[61]) e de dano relativo a programas ou outros dados informáticos, atenta a diversidade dos bens jurídicos tutelados e o objeto da ação de cada uma destas incriminações (num caso, são os dados informáticos e, noutro, é o sistema

59 Quanto ao que se deve entender por "forma grave ou duradoura", o legislador remete para uma apreciação casuística, dado que a gravidade e o caráter duradouro que justificam a agravação da pena aplicável por força do maior grau de ilicitude do facto terão de ser aferidos de acordo com as circunstâncias do caso concreto [cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime (em publicação)].

60 As funções sociais críticas são aquelas que se revelam essenciais para a subsistência da comunidade [cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime (em publicação)].

Como refere PEDRO VERDELHO, "Lei n.º 109/2009, de 15 de Setembro", *in* Comentário das Leis Penais Extravagantes, I, p. 514, na circunstância modificativa agravante prevista na alínea b) do n.º 5 do artigo 5.º da Lei n.º 109/2009, está em causa um agravamento da punição dos atos de sabotagem informática com consequências de enorme dimensão por força dos prejuízos que causam no exercício de funções sociais críticas, mas que podem não ser mensuráveis do ponto de vista económico. No fundo, esta circunstância modificativa agravante contempla os casos em que, por via do entravamento de um sistema informático é atingida, pelo menos, uma infraestrutura crítica, que é definida na alínea a) do artigo 2.º do Decreto-Lei n.º 62/2011, de 9 maio, como «*a componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções*». De referir, por último, que a enumeração de funções sociais críticas constante da alínea b) do n.º 5 do artigo 5.º da Lei n.º 109/2009 é meramente exemplificativa (cfr. BENJAMIM SILVA RODRIGUES, Da Prova Penal, IV, p. 158); assim, serão subsumíveis ao referido normativo os casos em que o sistema informático atingido apoie atividades como redes de abastecimento de energia, gás ou água, segurança aérea, sistemas de comunicações das polícias, hospitais, serviços de emergência médica, serviços públicos que emitam documentos, certidões, etc., os sistemas *Citius* e SITAF, o Portal do Governo, redes bancárias ou bolsistas (incluindo as redes de multibanco), etc.

61 Cfr. PEDRO VERDELHO/ROGÉRIO BRAVO/MANUEL LOPES ROCHA, Leis do Cibercrime, I, p. 253, e DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime (em publicação).

É discutido, na Doutrina e na Jurisprudência, qual é o bem jurídico tutelado pelo crime de sabotagem informática, encontrando-se duas correntes: uma primeira, que considera que é a integridade e o bom funcionamento dos sistemas informáticos e das comunicações eletrónicas (que subscrevemos); e uma segunda, que entende que é o património. Contudo, também aqui, uma abordagem mais detida desta questão não se justifica no âmbito do presente estudo.

informático)[62]. E existirá igualmente concurso efetivo entre o crime de sabotagem informática e os crimes que poderão estar em causa na fase de acesso ao sistema e aos dados.

62 Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime (em publicação).

5. A EXIGÊNCIA E O PAGAMENTO DO RESGATE

Bloqueado o acesso aos dados, a vítima receberá uma mensagem informando-a desse facto e do valor, prazo e forma de pagamento do resgate a ser pago para a "restituição" do acesso aos dados[63]. Tal mensagem é, muitas vezes, acompanhada da ameaça de que, se o resgate não for pago no prazo indicado, os dados serão definitivamente perdidos e/ou divulgados ao público, a entidades concorrentes e/ou às autoridades[64].

Os resgates são habitualmente pagos - por exigência dos agentes do crime - com criptomoedas[65], embora possam ser pagos de outras formas[66]. Deste modo, a conduta do agente constituirá (também) a prática de um crime de extorsão[67], p. e p. pelo artigo 223.º do Código Penal, nos termos do qual:

«*1 - Quem, com intenção de conseguir para si ou para terceiro enriquecimento ilegítimo, constranger outra pessoa, por meio de violência ou de ameaça com mal importante, a uma disposição patrimonial que acarrete, para ela ou para outrem, prejuízo é punido com pena de prisão até 5 anos.*

63 Cfr. RENAN CABRAL SAISSE, **Ransomware: "sequestro" de dados e extorsão digital, in** *http://direitoeti.com.br/artigos/Ransomware-sequestro-de-dados-e-extorsao-digital/* (acedido em 11/06/2019).

64 Cfr. DAVID WALL, "How big data feeds big crime", *in* Global History: A Journal of Contemporary World Affairs, 2018, p. 32, *in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3359972* (acedido em 12/06/2019).

JAMES A. SHERER/MELINDA L. MCLELLAN/EMILY R. FEDELES/NICHOLE L. STERLING, "Ransomware – Practical and legal considerations for confronting the new economic engine of the dark web", *in* Richmond Journal of Law & Technology, Volume XXIII, Fascículo 3, p. 13, *in https://jolt.richmond.edu/files/2017/04/Sherer-Final-May-1.pdf* (acedido em 13/06/2019), referem que os agentes do *Ransomware* costumam utilizar táticas psicológicas para forçar as vítimas a pagarem o regate exigido, incutindo-lhes sentimentos de culpa e de vergonha (*v.g.* acusando a vítima de ter cometido crimes e ameaçando-a com penas de prisão severas por alegadas visitas a *sites* de pornografia, pedopornografia, de sexo com animais ou abusos sexuais contra crianças) através do envio sistemático de dezenas ou centenas de mensagens até que a vítima pague o resgate.

65 Cfr. MÁRIO ANTUNES/BALTAZAR RODRIGUES, Introdução à Cibersegurança, p. 127, JAMES A. SHERER/MELINDA L. MCLELLAN/EMILY R. FEDELES/NICHOLE L. STERLING, "Ransomware – Practical and legal considerations for confronting the new economic engine of the dark web", *in* Richmond Journal of Law & Technology, Volume XXIII, Fascículo 3, p. 30, *in https://jolt.richmond.edu/files/2017/04/Sherer-Final-May-1.pdf* (acedido em 13/06/2019), RENAN CABRAL SAISSE, **Ransomware: "sequestro" de dados e extorsão digital, in** *http://direitoeti.com.br/artigos/Ransomware-sequestro-de-dados-e-extorsao-digital/* (acedido em 11/06/2019), MASARAH PAQUET-CLOUSTON/BERNHARD HASLHOFER/BENOÎT DUPONT, "Ransomware payments in the Bitcoin ecosystem", *in* Journal of Cybersecurity, 2019, pp. 1 e ss., *in https://watermark.silverchair.com* (acedido em 13/06/2019), e EUROPOL, IOCTA, 2018**,** pp. 24 e 58, *in www.europol.europa.eu/activities-services/main-reports/internet-organised-crimethreat-assessment-iocta -2018* (acedido em 08/06/2019).

66 Cfr. JAMES A. SHERER/MELINDA L. MCLELLAN/EMILY R. FEDELES/NICHOLE L. STERLING, "Ransomware – Practical and legal considerations for confronting the new economic engine of the dark web", *in* Richmond Journal of Law & Technology, Volume XXIII, Fascículo 3, p. 28, *in https://jolt.richmond.edu/files/2017/04/Sherer-Final-May-1.pdf* (acedido em 13/06/2019).

67 Se a vítima pagar o resgate, estaremos perante um crime consumado de extorsão; caso tal não suceda, estaremos perante um crime de extorsão na forma tentada, nos termos do artigo 22.º do Código Penal.

2 - Se a ameaça consistir na revelação, por meio da comunicação social, de factos que possam lesar gravemente a reputação da vítima ou de outra pessoa, o agente é punido com pena de prisão de 6 meses a 5 anos.

3 - Se se verificarem os requisitos referidos:

a) Nas alíneas a), f) ou g) do n.º 2 do artigo 204.º, ou na alínea a) do n.º 2 do artigo 210.º, o agente é punido com pena de prisão de 3 a 15 anos;

b) No n.º 3 do artigo 210.º, o agente é punido com pena de prisão de 8 a 16 anos.

4 - O agente é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias se obtiver, como garantia de dívida e abusando da situação de necessidade de outra pessoa, documento que possa dar causa a procedimento criminal.».

A essência do crime de extorsão reside em, mediante o uso de violência (física ou psíquica) ou de ameaça com um mal importante[68] (que podem ser dirigidas contra a vítima ou um terceiro, contra pessoas físicas ou coletivas[69]), constranger outra pessoa a realizar um ato de disposição patrimonial que acarrete um prejuízo patrimonial para ela ou para um terceiro, podendo esse ato consistir num *dare* (*v.g.* entregar dinheiro ou outro bem patrimonial), num *facere* (*v.g.* resolver um contrato ou renunciar a uma herança) ou num *non facere* (*v.g.* não reclamar um crédito ou não resolver ou denunciar um contrato)[70].

Assim, ao exigir o pagamento de um resgate para "restituir" o acesso aos dados (e, eventualmente, ao sistema informático), sobretudo se essa exigência for acompanhada da ameaça de que, se o resgate não for pago, os dados serão irremediavelmente perdidos e/ou divulgados ao público, a entidades concorrentes e/ou às autoridades, o agente está a constranger a vítima, através de uma ameaça com um mal importante, a realizar um ato de disposição patrimonial que lhe causa um prejuízo.

Tutelando o crime de extorsão o património[71] e a liberdade de decisão e de ação[72], existe concurso efetivo entre o crime de extorsão e os crimes de dano relativo a programas ou outros

68 Onde se inclui, por exemplo, a revelação de factos que possam lesar gravemente a reputação da vítima ou de um terceiro (*v.g.* o cônjuge ou um familiar próximo).
69 No que tange à violência contra coisas, a conduta só será típica se a violência contra coisas for um meio de exercer violência psíquica sobre a vítima (cfr. PINTO DE ALBUQUERQUE, Comentário do Código Penal, p. 614).
70 Cfr. PINTO DE ALBUQUERQUE, Comentário do Código Penal, pp. 613-614, e TAIPA DE CARVALHO, "Artigo 223º", *in* Comentário Conimbricense do Código Penal, I, 2.ª Edição, pp. 340 e 343-344.
71 Cfr. TAIPA DE CARVALHO, "Artigo 223º", *in* Comentário Conimbricense do Código Penal, I, 2.ª Edição, p. 343, e PINTO DE ALBUQUERQUE, Comentário do Código Penal, p. 613.
72 Cfr. TAIPA DE CARVALHO, "Artigo 223º", *in* Comentário Conimbricense do Código Penal, I, 2.ª Edição, p. 343.

dados informáticos, sabotagem informática, acesso ilegítimo e falsidade informática[73], o mesmo sucedendo quanto ao crime de ofensa à integridade física qualificada[74]. Quanto ao crime de coação ou de coação agravada, sendo o crime de extorsão uma forma especial (decorrendo a especialidade de a conduta coagida se traduzir num prejuízo patrimonial para a vítima[75]) do crime de coação[76], existe uma relação de concurso aparente, por especialidade, sendo o agente punido pelo crime de extorsão[77]; todavia, no caso do *Ransomware*, nas situações em que o agente tenha obtido as credenciais de acesso ao sistema informático mediante a prática de um crime de coação, a vítima da coação será tendencialmente (se não mesmo necessariamente) uma pessoa diversa da pessoa que é vítima da extorsão, pelo que existirá uma relação de concurso efetivo, não sendo possível a existência de crime continuado, por estarem em causa (também) bens jurídicos de natureza pessoal (*in casu* a liberdade de ação e de decisão)[78].

73 Cfr. DUARTE RODRIGUES NUNES, Os crimes previstos na Lei do Cibercrime (em publicação).
74 Cfr. PINTO DE ALBUQUERQUE, Comentário do Código Penal, p. 616.
75 Cfr. TAIPA DE CARVALHO, "Artigo 223º", *in* Comentário Conimbricense do Código Penal, I, 2.ª Edição, p. 340, e SIMAS SANTOS/LEAL-HENRIQUES, Código Penal Anotado, Volume III, 4.ª Edição, p. 1024.
76 Cfr. SIMAS SANTOS/LEAL-HENRIQUES, Código Penal Anotado, Volume III, 4.ª Edição, p. 1024, TAIPA DE CARVALHO, "Artigo 223º", *in* Comentário Conimbricense do Código Penal, I, 2.ª Edição, p. 340, e PINTO DE ALBUQUERQUE, Comentário do Código Penal, p. 616.
77 Cfr. PINTO DE ALBUQUERQUE, Comentário do Código Penal, p. 616, e TAIPA DE CARVALHO, "Artigo 223º", *in* Comentário Conimbricense do Código Penal, I, 2.ª Edição, p. 350.
78 Cfr. n.º 3 do artigo 30.º do Código Penal.

6. CONCLUSÕES

i) O *Ransomware* pode ser considerado enquanto tipo de *malware* e enquanto fenómeno criminoso ou atividade criminosa.

ii) Enquanto tipo de *malware*, o *Ransomware* é um tipo de *malware* desenvolvido com a finalidade de o agente do crime ter acesso a sistemas informáticos e aos dados neles armazenados sem conhecimento do respetivo titular com o objetivo de encriptar os dados e impedir o seu titular de lhes aceder para, posteriormente, exigir o pagamento de uma determinada quantia para recuperação do acesso aos dados.

iii) Enquanto fenómeno criminoso ou atividade criminosa, o *Ransomware* consiste numa atividade que se consubstancia, numa primeira fase, no acesso ilegítimo a sistemas informáticos[79] e a dados informáticos[80] alheios, para, numa segunda fase, bloquear os dados informáticos armazenados no sistema informático e impedir o seu titular de lhes aceder (podendo igualmente entravar esse sistema) e, numa terceira fase, exigir o pagamento de uma quantia em dinheiro para que os dados fiquem novamente acessíveis para o seu titular; caso o resgate não seja pago, o titular ficará definitivamente privado desses dados, que poderão ser tornados públicos ou vendidos a terceiros.

iv) A nossa ordem jurídica não possui uma incriminação específica do *Ransomware*, havendo que tentar subsumir a conduta do(s) agente(s) a algum dos tipos de crime previstos na lei.

v) Numa primeira fase, o agente do crime envidará esforços para conseguir aceder ao sistema informático-alvo e aos dados informáticos-alvo, mas, não possuindo, na maior parte das vezes, as credenciais necessárias (por exemplo, a *password*) para aceder ao sistema ou aos dados, é frequente e, para as obter, irá enviar à vítima ou a um seu colaborador um *e-mail* falso simulando ter sido enviado por uma pessoa conhecida da vítima ou por uma entidade legítima, convidando-o(a) a baixar um dado ficheiro, abrir um anexo, clicar e abrir um *link*, etc., o que, sendo feito, permite a instalação *sub-reptícia* de um *malware* que permitirá ao agente aceder ao sistema ou aos dados.

vi) A criação/envio do *e-mail* falso e a inserção das credenciais de acesso de um terceiro constitui a prática de um crime de falsidade informática.

---

79 Na aceção da alínea a) do artigo 2.º da Lei n.º 109/2009, de 15 de setembro.
80 Na aceção alínea b) do artigo 2.º da Lei n.º 109/2009.

vii) Se, para obter as credenciais de acesso, o agente recorrer à violência ou à ameaça com um mal importante, praticará também um crime de coação simples ou agravada, em concurso efetivo, se for o caso, com um crime de ofensa à integridade física grave.

viii) Ao aceder ilegitimamente ao sistema e aos dados, o agente comete um crime de acesso ilegítimo, p. e p. pelo artigo 6.º da Lei n.º 109/2009, sendo que, atenta a fenomenologia do *Ransomware*, a conduta tenderá a ser qualificada, se não nos termos do n.º 4, pelo menos nos termos do n.º 3.

ix) Existe concurso efetivo entre os crimes de acesso ilegítimo e de falsidade informática e entre esses crimes e os crimes de coação e de ofensa à integridade física grave.

x) Ao bloquear o acesso aos dados, tornando-os inacessíveis até que seja pago o resgate, o agente comete um crime de dano relativo a programas ou outros dados informáticos, sendo que, pela fenomenologia do *Ransomware*, a conduta tenderá a ser qualificada, nos termos do n.º 4 ou do n.º 5 desse preceito.

xi) Se, do bloqueio do acesso aos dados resultar também, pelo menos a título de dolo eventual, o entravamento do sistema, o agente cometerá igualmente um crime de sabotagem informática, sendo que, pela fenomenologia do *Ransomware*, a conduta tenderá a ser qualificada nos termos do n.º 4 ou do n.º 5 desse preceito.

xii) Existe concurso efetivo entre os crimes de dano relativo a programas ou outros dados informáticos e de sabotagem informática e entre esses crimes e os crimes de acesso ilegítimo, falsidade informática, coação e de ofensa à integridade física grave; todavia, no caso dos crimes de dano relativo a programas ou outros dados informáticos e de falsidade informática, a solução terá de ser casuística (existindo, nuns casos, concurso efetivo e, noutros, concurso aparente).

xiii) A exigência do pagamento do resgate (normalmente pago em criptomoedas) configura a prática de um crime de extorsão consumado (se o regate for pago) ou tentado (se o resgate não for pago).

xiv) Existe concurso efetivo entre o crime de extorsão e os crimes de dano relativo a programas ou outros dados informáticos, sabotagem informática, acesso ilegítimo, falsidade informática, coação (pois a vítima da extorsão é diversa da pessoa que é obrigada a fornecer as credenciais de acesso ao agente) e de ofensa à integridade física grave.

7. BIBLIOGRAFIA

Albuquerque, Paulo Pinto de – Comentário do Código Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, Universidade Católica Editora, Lisboa, 2008.

Andrade, Manuel da Costa – Consentimento e Acordo em Direito Penal, Coimbra Editora, Coimbra, 1991.

Antunes, Mário/Rodrigues, Baltazar – Introdução à Cibersegurança, A Internet, os aspetos legais e a análise digital forense, FCA, Lisboa, 2018.

Ascensão, José de Oliveira – "Criminalidade informática", *in* Direito da Sociedade da Informação, Volume II, pp. 203 e ss., Coimbra Editora, Coimbra, 2001.

August, Terrence/Dao, Duy / Niculescu, Marius Florin – Economics of Ransomware Attacks, *in* *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3351416* (acedido em 13/06/2019).

Bravo, Rogério – O Crime de Acesso Ilegítimo na Lei da Criminalidade Informática e na CiberConvenção, *in www.academia.edu/2039178/O_Crime_de_Acesso*

***Ilegi_timo_na_Lei_da_Criminalidade_Informa_tica_e_na_CiberConvencao* (acedido em 18/07/2018).**

Carvalho, Américo Taipa de – "Art. 154º", *in* Comentário Conimbricense do Código Penal, Parte Especial, Tomo I, 2.ª Edição, pp. 568 e ss., Coimbra Editora, Coimbra, 2012.

Carvalho, Américo Taipa de – "Art. 223º", *in* Comentário Conimbricense do Código Penal, Parte Especial, Tomo II, pp. 338 e ss., Coimbra Editora, Coimbra, 2012.

Costa, José Francisco de Faria – "Algumas reflexões sobre o estatuto dogmático do chamado "Direito penal informático"", *in* Direito Penal da Comunicação, Alguns escritos, pp. 103 e ss., Coimbra Editora, Coimbra, 1998.

Dias, Jorge de Figueiredo – Direito Penal, Parte Geral, Tomo I, 2.ª Edição, Coimbra Editora, Coimbra, 2007.

Europol – Carbanak/Cobalt Infographic, *in https://www.europol.europa.eu/publications-documents/carbanak/cobalt-infographic* (acedido em 04/07/2018).

Europol – Internet Organised Crime Threat Assessment 2018, *in www.europol.europa.eu/activities-services/main-reports/internet-organised-crimethreat -assessment-iocta-2018* (acedido em 08/06/2019).

Faria, Paula Ribeiro de – "Art. 144º", *in* Comentário Conimbricense do Código Penal, Parte Especial, Tomo I, 2.ª Edição, pp. 338 e ss., Coimbra Editora, Coimbra, 2012.

Glenny, Misha – Darkmarket, Como os Hackers se tornaram a nova Máfia, Civilização, Lisboa, 2012.

Marques, Garcia/Martins, Lourenço – Direito da Informática, 2.ª Edição Refundida e Actualizada, Almedina, Coimbra, 2006.

Martins, Lourenço – "Criminalidade informática", *in* Direito da Sociedade da Informação, Volume IV, pp. 9 e ss., Coimbra Editora, Coimbra, 2003.

Nováčková, Eliška – Current Cyberthreats and Relevant Legal Instruments in EU and Canada, *in* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3215960 (acedido em 11/07/2019).

Nunes, Duarte Rodrigues – O crime de falsidade informática, *in http://julgar.pt/o-crime-de-falsidade-informatica/* (acedido em 19/07/2019).

Nunes, Duarte Rodrigues – "O crime de dano relativo a programas ou outros dados informáticos", *in* Revista do Ministério Público, n.º 153, pp. 141 e ss., Lisboa, 2018.

Nunes, Duarte Rodrigues – Os meios de obtenção de prova previstos na Lei do Cibercrime, Gestlegal, Coimbra, 2018.

Nunes, Duarte Rodrigues – Os crimes previstos na Lei do Cibercrime (em publicação).

Paquet-Clouston,Masarah/Haslhofer, Bernhard/Dupont, Benoît – "Ransomware payments in the Bitcoin ecosystem", *in* Journal of Cybersecurity, 2019, pp. 1 e ss., *in https://watermark.silverchair.com/tyz003.pdf?token=AQECAHi208BE49O oan9kkhW_Ercy7Dm3ZL_9Cf3qfKAc485ysgAAAlAwggJMBgkqhkiG9w0BBwagggI9MIICO QIBADCCAjIGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQM_GII4a9WUXh0tSMdAg EQgIICA6PxkENBsKpmDo2YLVXUpZVvXRGHWvMEa1FdfRDdY3__n1lB2o 4VJaY8zaUigLQOtypFxdlzBeWmEs4kxoWhf1TNPwpkAWEpxyS2vRo1l4FgyQ7QPsYtF1WX RWpZyg-nh57o5c9b_wSz4o2s2UTxATSiTBR1lLK0w9gYxb1Cq8LIrE3ihbgwGnuw RuMca9Dc3E2Xo3cp2KigScnx_qD3VgQD0_ki82J6KFuUdoOEvw2VnYCFwwF7T8eF65flx8*

1IkNvfeX4BV5QyjCtT6jXg_Yu_pHqZ4_drH2shQlzqo7716ZxAlSwSQXgWaMtIyzJlczM3vp43hJ_uEX5_KlEG93o72zIRiSVVaAWLnNHsou5tdJ_V2pzmq26entn36lXQRYLHgzC0BUVnIvEy5K8GvLNfLb9GWY5xU5HlLlXmfSpEXO7iY8sIgNFiAyrg3TwLQI91u_NkTjmqHJVkX4-zV24Kf99ddLeXRzeQmLgckrfQJuZjQfHgn-yez61cXm011GuoMBET YF-iPLsbm7Ptsgfhdesg56MSIeL3bJGgpQcXO5vpf5XaFIX6vTk-4nz2HL9lY-7b-4unqTcS9RhsoDu6vUsOCBiP12wPYFmWluNEzB7OwBTtJbEA8DhJKAs68_GnlY3zhSN4rtoBF_dfvpbzxkCKiOTY3DnR92rhuD (acedido em 13/06/2019)

Rocha, Manuel António Lopes – "A lei da criminalidade informática (Lei n.º 109/01 de 17 de Agosto). Génese e técnica legislativa", *in* Cadernos de Ciência de Legislação, n.º 8 (Outubro-Dezembro 1993), pp. 65 e ss., Instituto Nacional da Administração, Lisboa, 1993.

Rodrigues, Benjamim Silva – Da Prova Penal, Tomo IV, Da Prova Electrónico-Digital e da Criminalidade Informático-Digital (Contributo para a Fundamentação de um Modelo Dinâmico-Reversivo de Ciência Forense Digital em sede de Investigação da Cyber-Criminalidade Informático-Digital e à Luz do Novíssimo Regime da Lei do Cibercrime Portuguesa), Rei dos Livros, Lisboa, 2011.

Saisse, Renan Cabral – **Ransomware: "sequestro" de dados e extorsão digital, *in*** *http://direitoeti.com.br/artigos/Ransomware-sequestro-de-dados-e-extorsao-digital/* (acedido em 11/06/2019).

Simas Santos, Manuel /Leal-Henriques, Manuel – Código Penal Anotado, Volume III, 4.ª Edição, Rei dos Livros, Lisboa, 2016.

Sherer, James A./McLellan, Melinda L./Fedeles, Emily R./Sterling, Nichole L. – "Ransomware – Practical and legal considerations for confronting the new economic engine of the dark web", *in* Richmond Journal of Law & Technology, Volume XXIII, Fascículo 3, pp. 1 e ss., *in* *https://jolt.richmond.edu/files/2017/04/Sherer-Final-May-1.pdf* (acedido em 13/06/2019).

Verdelho, Pedro – "Cibercrime", *in* Direito da Sociedade da Informação, Volume IV, pp. 347 e ss., Coimbra Editora, Coimbra, 2003.

Verdelho, Pedro – "Lei n.º 109/2009, de 15 de Setembro", *in* Comentário das Leis Penais Extravagantes, I, pp 505 e ss., Universidade Católica Editora, Lisboa, 2010.

Wall, David S. – "How big data feeds big crime", *in* Global History: A Journal of Contemporary World Affairs, 2018, pp. 29 e ss., *in* *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3359972* (acedido em 12/06/2019).

Artigos de imprensa

A atividade de *ransomware* diminuiu, mas ele ainda é uma ameaça perigosa, *in* *https://www.symantec.com/blogs/portugues/atividade-ransomware-diminuiu-ainda-ameaca-perigosa* (acedido em 17/07/2019).

Cibercriminosos mudam foco e ransomware cresce 167 vezes em 2016, *in* *http://computerworld.com.br/cibercriminosos-mudam-foco-e-ransomware-cresce-167-vezes-em-2016* (acedido em 04/07/2018).

Kaspersky lança três previsões sobre as ameaças para as criptomoedas em 2019, *in* *https://wintech.pt/w-news/26233-kaspersky-lanca-tres-previsoes-sobre-as-ameacas-para-as-criptomoedas-em-2019* (acedido em 14/07/2019).

Jurisprudência

- Tribunal da Relação de Coimbra

Acórdão de 17 de fevereiro de 2016 (Proc. 2119/11.TALRA.C2), *in www.dgsi.pt.*

- Tribunal da Relação de Lisboa

Acórdão de 25 de novembro de 2015 (Proc. 47/11.1TOLSB.L1-3), *in www.dgsi.pt.*

Acórdão de 7 de março de 2018 (Proc. 5481/11.4TDLSB.L1-3), *in www.dgsi.pt.*

Acórdão de 11 de abril de 2018 (Proc. 108/09.7XCLSB-3), *in www.dgsi.pt.*

- Tribunal da Relação do Porto

Acórdão de 14 de abril de 2004 (Proc. 0346424), *in www.dgsi.pt.*

Acórdão de 8 de janeiro de 2014 (Proc. 1170/09.8JAPRT.P2), *in www.dgsi.pt.*

AN INTRODUCTION TO BLOCKCHAIN TECHNOLOGY FROM A LEGAL PERSPECTIVE AND ITS TENSIONS WITH THE GDPR

DIOGO GUERREIRO DUARTE [1]

1 Research Trainee at Portucalense Institute for Legal Research (Oporto, Portugal). Contacts: diogo.gue.duarte@gmail.com

ABSTRACT

In this paper, we provide a brief overview of blockchain technology from a legal perspective, and its legal tensions with the General Data Protection Regulation (GDPR). The purpose of our study is to provide a first approach to help legal professionals, researchers, and students to better understand what is the blockchain technology and how it works, and what are its implications on data protection requirements, particularly in the allocation of responsibilities and in the data subject's rights. This study primarily focusses on the decentralized and immutable features of blockchain technology and the complexities and uncertainties it creates in respect to the centralized way in which the GDPR operates. Consequently, we also present a few solutions that can be implemented into the design of blockchain-based applications to achieve some of the GDPR's objectives.

Keywords: Blockchain; Distributed Ledger Technology; Encryption; Data Protection; General Data Protection Regulation (GDPR); EU Law.

RESUMO

No presente artigo pretendemos abordar numa breve visão geral a tecnologia blockchain de uma perspectiva legal e as suas tensões jurídicas com o Regulamento Geral de Proteção de Dados (GDPR). O objetivo do nosso estudo é procurar fornecer uma primeira abordagem para ajudar profissionais do mundo jurídico, investigadores e estudantes a compreenderem melhor o que é a tecnologia e como a *blockchain* funciona e quais são suas implicações nos requisitos de proteção de dados, particularmente na alocação de responsabilidades e nos direitos do titular dos dados. Concentrar-nos-emos, principalmente, nos recursos descentralizados e imutáveis da tecnologia *blockchain* e nas complexidades e incertezas que esta cria em relação à maneira centralizada pela qual o Regulamento Geral de protecção de dados (RGPD) opera. Concomitantemente, apresentaremos ainda algumas soluções que podem ser implementadas no *design* de aplicativos baseados em *blockchain* para alcançar alguns dos objetivos do RGPD.

Palavras-chave: *Blockchain*; Tecnologia Distributed Ledger; Criptografia; Proteção de Dados; Regulamento Geral de Proteção de Dados (RGPD); Legislação da UE.

TABLE OF CONTENTS

1. INTRODUCTION

Since the General Data Protection Regulation (GDPR) came into force, numerous questions have emerged in relation to its applicability to blockchain technology. At first sight, this innovative class of new technologies seems to be unable to comply with GDPR's requirements, due to its very immutable, decentralized and transparency-based nature, thus restraining its own development and, consequently, endangering the European digital market and its technological development.[1] At the same time, being the respect for human rights one of the most important core values of the European Union,[2] the protection of natural persons with regard to the processing of personal data is expressly established in the most relevant European Union's instruments, namely under the article 8 (1) of the Charter of Fundamental Rights and the article 16 (1) of the Treaty on the Functioning of the European Union (TFEU). In this respect, the development of the internal market and the promotion of human rights need to find a fair balance, allowing the European Union to achieve its economic objectives, without sacrificing the protection of human rights, and vice-versa.[3]

As we will observe through this study, GDPR implicitly assumes that data is controlled or processed by identifiable actors, in a centralized manner. On the contrary, blockchain-based applications where designed to operate in a decentralized manner, with multiple actors and participants within a widely distributed network. The non-linear operation of blockchain-based applications, in relation to the GDPR, gives rise to several tensions, which led to the idea that theirs is an incompatible relationship. In order to detail the nature of these tensions, the main focus of this study is identifying the key features of blockchain technology that might pose a challenge to the GDPR's requirement, in particular to the data subjects' rights and freedoms. Additionally, we will explore how blockchain-based applications can be used to help achieve GDPR's objectives.

To accomplish this analysis, we will firstly provide an overview on blockchain technology, highlighting its main characteristics both from a technical and a legal perspective.

1 Article 173 (1) of Treaty on the Functioning of the European Union.
2 Article 2 of the Treaty on European Union.
3 The objectives of the internal market are described, in a general manner, in the Article 3 (3) of the Treaty on European Union.

Once we have identified its main elements of blockchain-based applications, we will examine the different types of blockchains and the roles its participants can assume in each one of them. Subsequently, we will study in further detail the existent complexities and uncertainties this technology introduces in relation to the GDPR's requirements. Finally, we explore the technological solutions that may be incorporated into blockchain-based applications to comply with the GDPR and to help achieve the GDPR's objectives. In this particular regard, we provide two solutions that, once embodied into blockchain-based applications, may allow natural and legal persons to take full advantage of the blockchain technology, aiming to achieve a fair balance between the promotion and protection of human rights and the digital market development.

A final note must be addressed to state that compliance with the GDPR is not about technology itself, but rather, it is about how technology is used.[4] Despite recognizing the need to conduct a case-by-case analysis, this study aims to provide a general overview of the application of the GDPR's requirements to the various types of blockchain-based applications.

4 *See* Ibáñez, Luis-Daniel, O'Hara, Kieron and Simperl, Elena (2018), "On Blockchains and the General Data Protection Regulation", EU Blockchain Forum and Observatory, p. 29.

2. BLOCKCHAIN

In its historical context, the starting point of the blockchain technology can be traced back to 2008, when an individual (or a group) writing under the pseudonym Satoshi Nakamoto published a whitepaper intitled '*Bitcoin: A Peer-to-Peer Electronic Cash System*'.[5] In this whitepaper, Bitcoin emerges as a '*purely peer-to-peer version of electronic cash*'[6], that uses a decentralized network to enable irreversible transactions.[7] In this new open-source online currency system, based on a peer-to-peer network, transactions can be made between the holders of the currency directly with one another, without going through any intermediaries such as financial institutions.[8] As this system does not rely on third-parties to validate, safeguard, and preserve transactions, payments can be made immediately and without the extra fees that typically increase the cost of the transactions.[9] Additionally, Bitcoin also makes non-reversible payments possible, which is a distinct feature of its technology, considering that financial institutions and other intermediaries cannot avoid mediating disputes between transacting parties, which is why non-reversible transactions are not possible within a centralized trusted entity model.[10]

Although Bitcoin was not the first manifestation of the idea of a digital currency[11], it was the first realization of this concept, and the first digital payment system that successfully allowed its participants to make direct online transactions, without placing any trust towards a central authority, and also solved the '*double-spending*' problem without relying on a trusted third party.[12] (Briefly, on blockchain cryptocurrency's applications, the digital files representing a cryptocoin can be duplicated or falsified, thus being able to potentially be used

---

5 *See generally* Chang, Henry, (2017) "*Blockchain: Disrupting Data Protection?*", Privacy Law and Business International Report, November 2017; University of Hong Kong Faculty of Law Research Paper No. 2017/041.
6 *See* Nakamoto, Satoshi, (2008) "*Bitcoin: A Peer-to-Peer Electronic Cash System*", www.bitcoin.org, p. 1.
7 *See* Maurer, B., Nelms, T. C., & Swartz, L. (2013), "*When perhaps the real problem is money itself! the practical materiality of Bitcoin*", Social Semiotics, 23(2), p. 261.
8 *Ibid*.
9 This is what Nakamoto calls '*the cost of mediation*'. *See* Nakamoto S., (2008) supra note 3, p. 1.
10 *Ibid*.
11 The idea of a cryptographic currency dates to 1983. In his article, entitled '*Blind Signatures for Untraceable Payments*', the author David Chaum proposes an untraceable-payments system based on a blind-signatures system. This system can be described as follows: "*A single note will be formed by the payer, signed by the bank, stripped by the payer, provided to the payee, and cleared by the bank*". During the 90's, the initial blind-signatures system obtained some important contributions, such as allowing payments without the bank being online at the purchase time; allowing coins to be divided into smaller unites; and improving its overall efficiency. *See* D. Chaum (1983) "*Blind Signatures for Untraceable Payments, Advances in Cryptology*", Proceedings of the Springer-Verlag Crypto'82, Vol. 3, p. 202.
12 Before the creation of Bitcoin, several companies, such as DigiCash and Peppercoin, attempted to implement electronic cash protocols. *See* Crosby, M., Nachiappan, Pattanayak, P., Verma, S., and Kalyanaraman, V., (2016), "*Blockchain Technology: Beyond Bitcoin*", Applied Innovation Review, Issue No 2, p. 2. *See also* Nian, L., Chuen, D. (2015), "*Introduction to Bitcoin*", Handbook of Digital Currency, Chapter 1, pp. 9-11.

more than once – this flaw is termed *double-spending*.) More broadly, the importance of Bitcoin lies on its technological structure, as it materializes the first usage of blockchain technology.[13] In fact, Bitcoin was the first ever application of blockchain technology[14] and, for that reason, the two concepts are often confused with one another, although they differ in many other aspects. For instance, Bitcoin is a cryptocurrency that was basically created to simplify and increase the speed of transaction, without relying on the intervention of a central organization or a third party. As we will observe later in this section, blockchain technology is not limited to transactions of cryptocurrencies, as it can be used to transfer any type of data or information, and can be easily adapted to different types of business and purposes.[15] Overall, the relationship between these concepts is easily understood if we consider that '*blockchain is Bitcoin's backbone technology*'.[16]

However, defining and circumscribing the concept of blockchain technology is not a straightforward task. In the absence of a unique and consensual definition in the blockchain literature, many authors tend to use different criteria to define blockchain technology.[17] For instance, some authors define blockchain by stressing out its technical characteristics and core components; others try to comprise the essential features of blockchain into a generic definition; while there some who, based on a Bitcoin blockchain generic definition, introduce some of the most recent developments of this technology.[18] In our view, in order to define and

13 See Fabiano, N. (2018), "Blockchain and Data Protection: The Value of Personal Data", J. Systemics, Cybernetics & Informatics, p. 49.

14 As Sater refers, '*Bitcoin, a cryptocurrency and a protocol, was the first decentralized and permission-less peer-to-peer payment system to implement blockcha*in'. *See* Sater, Stan (2017), "Blockchain and the European Union's General Data Protection Regulation: A Chance to Harmonize International Data Flows", Social Science Research Network, p.19. *See* also Bonneau, J., Miller, A., Clark, J., Narayanan, A., A. Kroll, J., and Felten, E., (2015) "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies", IEEE Symposium on Security and Privacy, p. 2; and Schwerin, Simon (2018) "Blockchain and Privacy Protection in the Case of the European General Data Protection Regulation (GDPR): A Delphi Study", The Journal of The British Blockchain Association, Vol. 1, Issue 1, p. 20.

15 '[Contrary to Bitcoin] *Blockchain technology itself is non-controversial and has worked flawlessly over the years and is being successfully applied to both financial and non-financial world applications*', see Crosby, M., Nachiappan, Pattanayak, P., Verma, S., and Kalyanaraman, V., (2016), supra note 12, p. 8.

16 *Ibid.* p. 17.

17 As Schwerin identifies, the blockchain technology is currently under development, which makes it difficult to establish a precise and clear definition of its concept. In the author's view, it is possible to decompose the definition of blockchain into three layers: 1) the datalogical layer, which refers to the cryptographic functions that are used to store all transactions; 2) the infological layer, which perspectives the blockchain definition as a series of inputs and outputs between accounts that are stored in a public ledger; and 3) the essential layer, which sees transactions as commitments and economic events. *See* Schwerin, S., (2018), supra note 14, p. 21.

18 For a technical definition of blockchain and its core components, *see* Cate, Fred H.; Kuner, Christopher; Lynskey, Orla; Millard, Christopher; Ni Loideain, Nora; and Svantesson, Dan Jerker B., (2018), "*Blockchain versus Data Protection*", International Data Privacy Law, Volume 8, Issue 2, p. 103. For a broader definition of blockchain, *see* Ibáñez, Luis-Daniel, O'Hara, Kieron and Simperl, Elena (2018), supra note 4, p. 1. For a Bitcoin blockchain based definition and its subsequent developments, *see* Wright, Aaron and De Filippi, Primavera,

explain what blockchain is, we must begin by acknowledging that there is not one single blockchain technology, but, on the contrary, there is an entire class of technologies that present different technical and governance structures.[19] Thus, any attempt to define the concept of blockchain, if it goes beyond the core components common to all varieties of this technology, will fail to recognize the existence of other blockchain types. As a mere example, the typical definition of blockchain includes a reference to the resource-intensive consensus mechanism, which is used by miners to validate pending datasets and form news blocks on the chain.[20] While this feature is common among DTLs (distributed ledgers technology), the same cannot be said about the centralized trusted third-party models like private blockchain-based applications in which there is only a single entity that manages the entire blockchain. In this context, a more rigorous and realistic approach to the concept of blockchain technology requires, in the first place, the consideration of its core components. Only then it is possible to introduce and analyze the different technical and governance structures blockchain can assume, which are crucial to measure the different impact those structures have on data protection[21].

2.1 Core components of blockchain technology

Taking into account the aforementioned difficulties of producing a unanimous definition, blockchain can be generally described as a specific type of database that '*uses certain cryptographic functions* [mathematical functions/algorithms used in cryptography, *i.e.* the study and construction of protocols that prevent third parties from accessing private communications and transactions] *to achieve the requirements of data integrity and identity*

(2015) "Decentralized Blockchain Technology and the Rise of Lex Cryptographia", Social Science Research Network, pp. 1-4. Available at SSRN: https://ssrn.com/abstract=2580664

19 *See* Finck, Michèle (2019), "*Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?*", Panel for the Future of Science and Technology, European Parliamentary Research Service, Scientific Foresight Unit, PE 634.445, p. 3.

20 As we will see in the sections below, miners or validating nodes are one of the three participants on blockchain, which are responsible for assembling datasets into blocks and broadcast those blocks to other nodes across the peer-to-peer network, in order to validate the new block and add it on the chain.

21 In this issue, we follow the approach taken by Jean Bacon et al., who expressly acknowledge that this approach is more useful as "*(…) a lot of existing material assumes that readers are familiar with the underpinning technologies. Further, some sources fail to distinguish between the core components of blockchain and the various ways in which the technology could be applied*". *See* Bacon, Jean and Michels, Johan David and Millard, Christopher and Singh, Jatinder, (2017) "Blockchain Demystified", Queen Mary School of Law Legal Studies Research Paper No. 268/2017, p. 3.

authentication'.[22] These two core components of blockchain technology – data integrity and identity authentication – allow it to create a persistent and tamper-evident record of the dataset and authenticate the parties associated with it.[23] In this section, in order to explain how blockchain works and what are its core components in a simple manner, we will use the train's metaphor, in which the train represents the whole blockchain, each carriage characterizes a block of the chain, and the passengers symbolize single data items.

2.1.1. Data Integrity

The early applications of blockchain, such Bitcoin, were created to operate in a trustless environment, where the blockchain should not be managed by any central party, but instead stored in a distributed manner across the peer-to-peer network, in which each node holds an updated copy of the ledger of transactions.[24] In the same way the distributed peer-to-peer network is essential to overpass the inexistence of a central entity, the cryptographic hash functions are essential to safeguard the integrity of the transactions.[25] In practice, hash functions not only create a tamper-evident record of the transactions, but also guarantees that they are "*computationally impractical to reverse*".[26] Bitcoin and other blockchain applications use hash functions to generate a unique hash value to the input data item, which consists of a string of digits with a fixed length.[27] The hash value is used to prove the integrity of a data item, in that any change to the original data item will generate a different and unrelated hash value that allows blockchain's participants to detect if any attempt to tamper the data has occurred. For this particular reason, it is commonly said that the hash value of a data item works as its fingerprint, in that this value is unique.[28] Besides this particular characteristic, the hash functions are irreversible, in the sense that is not possible to use the hash value to recreate the original input of a particular data item. Revisiting the train's metaphor, the hash functions

22 *See* Bacon, J.; Michels, J.; Millard, C.; Singh, J. (2017), supra note 21, p. 4.
23 In order to include all the possible types of data blockchain can incorporate, the term 'dataset' is used in this study in a broad manner. Regarding the early applications of blockchain, such as cryptocurrencies, this term refers to the ledger of transactions. However, as other applications of blockchain are being currently explored, the term dataset can also include different types of data, such as land registers.
24 *See* Nakamoto, Satoshi, (2008), supra note 3, p. 1.
25 Bitcoin uses SHA-256. This cryptographic hash function requires validating nodes (or miners) to solve a cryptographic puzzle, in which they need to find a block, whose SHA-256 hash is less than a target value. In the Bitcoin context, the miners try random nonces (an arbitrary number that can be used just once in a cryptographic communication) until they find a solution, that is then broadcasted to the entire network in order to be confirmed by the other nodes. For more details, *see* Bonneau, J., Miller, A., Clark, J., Narayanan, A., A. Kroll, J., and Felten, E., (2015) supra note 14, pp. 2-5.
26 *See* Nakamoto, Satoshi, (2008), supra note 3, p. 2.
27 *See* Bacon, J.; Michels, J.; Millard, C.; Singh, J. (2017), supra note 21, p. 6.
28 *See* Wright, Aaron and De Filippi, Primavera, (2015), supra note 18, p. 7.

works, in this specific context, as a way to verify that passengers have a valid ticket to enter the train and that the ticket was not tampered or falsified in any way, as it is unique and only can be used by those particular passengers.

Beyond single transactions and data items, the hash functions also play an important role in making large data structures, which contain multiple transactions or data items, tamper-evident, by using hash pointers. On blockchain, those structures are commonly known as blocks, and each block contains a record of numerous individual transactions or other data items. In order to prove the integrity of the blocks, including its content and sequence, hash pointers link the blocks together, by putting into a hash function the combination of the data of each block with the hash value of the previous block. This creates a block's hash value that will be included in the next block alongside with a list of transactions or datasets and other metadata.[29] The result is a tamper-evident chain of blocks, in which any attempt to modify a block's content, will immediately break the link between blocks, allowing any fraudulent interfering to be easily spotted.[30]

In our train's metaphor, in which a carriage represents a block of transactions or other data items, the function of the 'hash pointers' is to link all the individual carriages that form the train in their proper order. In order to ensure the integrity of the train, each carriage includes a number that represents the previous one, which is generated through the combination of the carriage number and the passengers' tickets numbers. In case a modification occurs, whether regarding to passengers' tickets or to the carriage itself, the link with the other carriages will break automatically, showing that something wrong happened with any particular carriage or a passenger's ticket.

Early blockchain applications were conceived to be practically immutable and irreversible, recording and linking all the transactions into a chain of blocks. From an early stage, a concern about storage space was emerged, since the more transactions occur, the more the database grows.[31] The use of a Merkle tree provided a solution to both storage space and data verification[32]. In general, a Merkle tree is a hash-based data structure that contains the

29 As Jean Bacon *et al.* correctly identify, a block consists of two main parts: a '*block body*', that contains a list of all transactions that a block holds; and a '*block header*', that is composed by the hash of the previous block and some metadata, such as a timestamp. *See* Bacon, J.; Michels, J.; Millard, C.; Singh, J. (2017), supra note 21, pp. 7-8. *See* also Bonneau, J., Miller, A., Clark, J., Narayanan, A., A. Kroll, J., and Felten, E., (2015), supra note 14, pp. 4-5.

30 However, this only mitigates the risk of data being modified by an attacker, as it is virtually possible to re-hash the blocks and reconstruct the chain if the attacker holds the majority of the computational power on the network.

31 *See* Nakamoto, Satoshi, (2008), supra note 3, p. 4.

32 *Ibid*.

combination of the hash values of the individual transactions. In practice, the hash values of individual transactions are paired and put into a hash function in order to generate new hash values. This process is successively repeated until the last hash value – also known as the Merkle root – is found.[33] Each block contains a Merkle root, which represents a summary of all transactions a block holds. Besides requiring less space to store data and using fewer resources, the Merkle tree system makes it easier to verify the integrity of transactions and to check if a transaction has been included in a block without having to download the entire ledger of transactions.[34]

2.1.2. Identity Authentication

Presently, a large number of transactions related to the most diverse economic activities are still executed using financial intermediaries, such a financial institution or a bank. In this context, one of the main duties of a financial institution is to correctly identify the parties involved in a transaction and to ensure the content of the transaction is accurate. As mention above, early applications of blockchain, such as Bitcoin, were designed to operate in a trustless environment, *i.e.* without the intervention of a trusted third-party. However, blockchain still needs to identify and authenticate the parties involved in any transaction, before storing it into a block. To achieve this purpose, blockchain technology relies on a security method known as public key infrastructure (PKI).[35] This security method is used to implement strong authentication by generating a key pair containing a public and a private key, a signing algorithm, and a validation function that checks the digital signatures' validity.[36]

---

33 In order to observe how a Merkle root is obtained, let us consider the following example. Imagine that a block holds eight transactions (Tx), in which eight persons sent a certain amount of Bitcoin to other eight persons. As we mentioned above, each transaction (Tx1, Tx2, …, Tx8) is put into a hash function generating a unique hash value (h1, h2, …, h8). These hash values are then paired and put into a new hash function: (h1+h2) = h12; (h3+h4) = h34; (h5+h6) = h56; and (h7+h8) = h78. As a result, we have compressed the eight transactions into four hash values. However, to achieve a final hash value – a Merkle root – the process must continue. Thus, the four hash values are paired and put into a new hash function: (h12+h34) = h1234; (h56+h78) = h5678. The process repeats itself one last time, resulting in a Merkle root: (h1234+h5678) = h12345678. This hash value (h12345678) is then added to the block header. In case a single transaction is modified or tampered in any way, this will generate a completely different hash value, modifying, by consequence, the Merkle root. In this way, it becomes easier to detect any change in the block. For a visual explanation of this concept, *see* Bashir, I., (2017), "*Mastering blockchain*", Packt Publishing Ltd., pp. 174-177.

34 Although storage space is not considered to be a problem on blockchain, as the Moore's Law predicts that the computer capacity will be enough to store all the data inside blockchain, the use of the Merkle tree is undoubtedly a more manageable way to process large amounts of data. *See* Nakamoto, Satoshi, (2008), supra note 3, p. 4.

35 *See* Nian, L., Chuen, D. (2015), supra note 12, pp. 15-17.

36 *See* Bacon, J.; Michels, J.; Millard, C.; Singh, J. (2017), supra note 21, p. 9.

As all the transaction records on blockchain are signed before being included in blocks, the PKI is mainly used to establish the digital identity of a user and to create digital signatures. The public and private key can be used to encrypt and decrypt data that has been respectively encrypted or decrypted using one of these keys. Thus, to prove its identity or to sign a transaction or any other data item, a user can encrypt data using her private key and provide the associated party with the public key. If the associated party can successfully decrypt the data using the public key provided by the user, she can be confident that the transaction, or any other data item, originated from that particular user.[37]

The train's metaphor we used to explain the data integrity component, when applied to the identity authentication component, works in the following way: imagine it is only possible for a passenger to enter the carriage with an coded ticket that must be acquired on a specific platform. When creating a profile on that platform, the passenger receives a private password to login and a public password that she must give alongside the ticket before entering the carriage. An officer then uses the public password to confirm that the ticket belongs to that passenger. In case the public password provided by the passenger allows the officer to successfully scan the train ticket, her entity is proved, and she is accepted on the carriage.

2.2 Types of blockchain

On its historical context, cryptocurrencies were the first application of blockchain technology, which came into existence to surpass the '*inherent weaknesses of the trust based model*'[38], namely the fraud percentage that is accepted as unavoidable on such a model and, more specifically, the transactions' time-length and costs that costumers support when using third parties to process electronic payments. Consequently, the early applications of blockchain technology were designed to operate without a trusted third party. However, an important question arises from this paradigm: who controls the blockchain?

The question can be divided into the following two questions: who can store copies of the blockchain, and who can propose new blocks to be added to the blockchain?[39] As different

37 Unless the private key has been compromised by any attack on the user account or computer devices. *Ibid*.
38 *See* Nakamoto, Satoshi, (2008), supra note 3, p. 1.
39 *See* Bacon, J.; Michels, J.; Millard, C.; Singh, J. (2017), supra note 21, p. 10.

answers can be given, the design of the platforms using blockchain technology can vary significatively, creating different types of blockchain applications. Although the blockchain's design can present a wide spectrum,[40] to make the concept easier to understand blockchain types are usually segmented into private or public, and permissionless or permissioned databases.[41]

The criterion to differentiate private or public blockchains can be found by observing the way participants join the network. In this respect, while public blockchains are open to any person or entities that desire to join the peer-to-peer network, on another hand, private blockchains only allow pre-selected participants to join their peer-to-peer network. The pre-selected criterion is also used to differentiate permissionless and permissioned blockchains. In the first, any person or entity can participate in the consensus mechanism, having the possibility to add new blocks into the chain. On permissioned blockchains, only the pre-selected entities are authorized to add new blocks into the chain. [42]

For the purposes of our study, our analysis will focus next on the structure of both public, private and consortium blockchains, as the role of its participants are crucial to consider the impact these blockchain types have on data protection.

2.2.1 Public and permissionless blockchains

Cryptocurrencies are perhaps one the most widely known application of blockchain technology. As Jean Bacon *et al.* (2017) affirm, Bitcoin *'shaped the public perception of what a blockchain is*'.[43] Indeed, Bitcoin has an enormous importance to the development of blockchain technology, not only because it was the first digital currency to be successfully implemented, but more importantly, it allowed direct transactions to be made without the intervention of a trusted third party.[44] In order to operate in a trustless environment, Bitcoin's design relies in the combination of three main components: a decentralized peer-to-peer network (P2P network); a consensus mechanism; and a series of cryptographic functions.[45]

---

40 In its book, the author Irman Bashir provides a list of different blockchain types, which includes public; private; and semi-private blockchain; sidechains; permissioned ledger; shared ledger; fully private and proprietary blockchains; tokenized blockchains; and tokenless blockchains. *See* Bashir, I., (2017), supra note 33, pp. 32-34.
41 *See* Schwerin, Simon, (2018), supra note 14, p. 25.
42 *Ibid*.
43 *See* Bacon, J.; Michels, J.; Millard, C.; Singh, J. (2017), supra note 21, p. 5.
44 *See* Schwerin, Simon, (2018), supra note 14, p. 20.
45 *See* Schwerin, Simon, (2018 supra note 14, p. 22. *See* also Bonneau, J., Miller, A., Clark, J., Narayanan, A., A. Kroll, J., and Felten, E., (2015) supra note 14, pp. 2-9.

In the beginning of this section (*2.1. Core components of blockchain technology*), we analyzed how cryptographic functions work in blockchain environment. As this core component is common to the different types of blockchain, we are going to examine the other core components of public and permissionless blockchains, using Bitcoin as example.

Although the P2P network is often described as the least innovative of the three main components of Bitcoin, using our train's metaphor, this component is the engine of blockchain.[46] There are three type of participants in Bitcoin's blockchain: user, nodes and miners. Each one of these participants has a different role on the P2P network. *Users* are the persons or the entities that use Bitcoin to make transactions, *i.e.* to buy or sell bitcoins. On the user's level, Bitcoin is open and permissionless, which means that anyone can participate by simply buying a bitcoin hardware wallet, running an open source code on the computer, or using online software wallet services.[47] The *nodes*' role is of fundamental importance on Bitcoin's platforms, as they not only accept and validate transactions broadcast by the miners, but they also discover and maintain connections with other nodes to whom they send an update copy of the ledger.[48] On the nodes' level, Bitcoin is also open and permissionless, as anyone can download and run the Bitcoin's appropriate software and start storing the blockchain archive into the computer. Finally, the *miners* are the Bitcoin's participants, who assemble transactions into blocks and broadcast those blocks to the entire P2P network, according with a consensus mechanism that we will analyze next. Regarding the mining process, an interesting feature of Bitcoin architecture is that it incentivizes miners to perform the task of adding new blocks to the blockchain through an economic reward, which is also the way Bitcoin puts new coins into circulation.[49] On the miner's level, Bitcoin platform is, once again, open and permissionless, which means that anyone can be a miner.

As the open and permissionless types of blockchain do not rely on a single centralized party, the P2P network is crucial to maintain the integrity of the ledger, in the sense that even if any interference with the ledger occurs, the rest of the P2P network still has a valid copy of

---

46 *Ibid*.

47 Regardless of the way the user has chosen to join the P2P network, a public-private key pair is generated, allowing her to start using Bitcoin's platform. A user can start trading by either receiving bitcoins from another user or buying bitcoins from online exchanges. *See* Bacon, J.; Michels, J.; Millard, C.; Singh, J. (2017), supra note 21, p. 11.

48 See Bonneau, J., Miller, A., Clark, J., Narayanan, A., A. Kroll, J., and Felten, E., (2015), supra note 14, p. 5, ('By default, each node attempts to make eight outgoing connections and is prepared to receive up to 125 incoming connections').

49 The miners can also be rewarded through transactions fees, which are normally used by the users to incentive miners to prioritize their transactions. In practice, a transaction fee is the difference between the input and output values that users allow miners to retain. *See* Nakamoto, Satoshi, (2008), supra note 3, p. 4.

the ledger, which will be used by the majority of the nodes and miners to create, validate and add new transactions and blocks into the chain. Because the P2P network operates in a decentralized manner, it increases the resilience of the blockchain platform, as there is no single point of failure that can be targeted with a denial of service attack.[50] However, to operate properly, namely to allow new blocks to be added to the blockchain, it is required that all the nodes and miners in the network hold an updated and synchronized copy of the ledger.[51] To this end, open and permissionless blockchain such as Bitcoin have implemented a consensus mechanism.

The Proof-of-Work (PoW) is one of the most well-known and the most used consensus mechanisms on public and permissionless blockchains. PoW is a protocol that is used to validate the data (or transactions) and form new blocks on the chain[52]. One key feature of the PoW is its asymmetry, as the work is difficult to produce, since it requires increasing amounts of computational power to decipher the cryptographic puzzle specifically created to be solved by the means of brute force calculation,[53] but is easy to be verified by all the other nodes, who can create consensus on the solution broadcasted to the whole P2P network by the first node that solved that particular cryptographic puzzle. Once the solution has been confirmed by all the other nodes and consensus has been achieved, the new block can then be appended to the longest chain.

Although the PoW is the most common consensus mechanism, there are many other types of mechanisms, such as the Proof of Stake (PoS), Byzantine fault-tolerant variants (BFT), Proof of Elapsed Time (PoET), and Algorand.[54] Apart from the specific particularities of each one of them, the consensus mechanisms are used to serve two different purposes simultaneously. On one hand, by checking the current state of the blockchain on a regular basis, the mechanisms perform a process that aims to mitigate the creation of forks into the blockchain

50 *See* Bacon, J.; Michels, J.; Millard, C.; Singh, J. (2017), supra note 21, pp. 12-13.
51 *See* Lyons, T., Courcelas, L., and Timsit, K. (2018), "Blockchain and the GDPR", European Union Blockchain Observatory and Forum, p. 14.
52 The SHA-56 is one of the most used proof-of-work schemes and it was introduced by Bitcoin. This cryptographic hash function requires validating nodes (or miners) to solve a cryptographic puzzle, in which they need to find a block, whose SHA-256 hash is less than a target value. In the Bitcoin context, the miners try random nonces (an arbitrary number that can be used just once in a cryptographic communication) until they find a solution, that is then broadcasted to the entire network in order to be confirmed by the other nodes. For more details, *see* Bonneau, J., Miller, A., Clark, J., Narayanan, A., A. Kroll, J., and Felten, E., (2015), supra note 14, pp. 2-5.
53 *See* also Ibáñez, Luis-Daniel; O'Hara, Kieron; and Simperl, Elena (2018), supra note 4, pp. 2-3.
54 *See* Truong, N., Sun, K., Lee, G., Guo, Y. (2019) "GDPR-Compliant Personal Data Management: A Blockchain-based Solution", IEEE transaction on information forensics and security, p. 2.

and their frequency. This process is frequently referred to as the '*fork choice rule process*'.[55] On the other hand, the consensus mechanisms are used to ensure the majority of the nodes on the network agree on the legitimacy and validity of the transactions that a proposed new block contains, avoiding the malicious nodes to broadcast their own blocks. In general, the consensus mechanism allows nodes to audit the entire blockchain by constantly checking all the transactions, which significantly reduces the risk of various attacks.[56]

Once added to the blockchain, each block is computationally impractical to modify, which means transactions are recorded into blockchain on a permanent basis. In order to successfully modify a block, a validating node would need the majority of the computational power within the P2P network to do it.[57] Even if a node could successfully modify a dataset on a block, it would need to re-hash the subsequent blocks in the chain, since any modification to the dataset would automatically break the blockchain.[58] Additionally, and since the chain with the most combined computational difficulty is considered the valid one, an attacker would needed to control the addition of new blocks and, thus, use the PoW much faster than the rest of the P2P network. For these reasons, public and permissionless blockchains are considered to have a strong security feature and a *'51% attack*' is unlikely to happen, although the '*mining pools*' (*i.e.* a group of two or more miners that work together) could be virtually able to concentrate 51% of the computational power of the P2P network. [59]

2.2.2 Private and permissioned blockchains

As we mention above, the public and permissionless blockchains were designed to operate in a trustless environment, where anyone can participate either by proposing, verifying or adding new data to the blockchain. Although these features fit the purposes of early

55 From time to time, two blocks can be created simultaneously, generating a fork on the blockchain. During a fork, one of the blockchain branches will be discarded since the validating nodes (or miners, in the case of Bitcoin) will converge on the other branch. During the time a fork subsists, the blocks of both branches will be apparently included in the longest chain. The '*length*' of the entire blockchain refers not to the one with the most blocks, but to the chain that has the most combined computational difficulty. This prevents some node from forking the chain and creating many low-difficulty blocks, which otherwise would be accepted by the network as the longest chain.
56 *See also* Nian, L., Chuen, D. (2015), supra note 12, pp. 22-25.
57 Since the attacker must have most of the computational power of the entire P2P network, the attack to a public and permissionless blockchain that uses the PoW became known as the '*51% attack*'. For more details on this kind of attacks and their feasibility, *see* Bacon, J.; Michels, J.; Millard, C.; Singh, J. (2017), supra note 21, pp. 17-18.
58 Nakamoto S., (2008), supra note 3, p. 1 ('The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work').
59 S*ee* Bacon, J.; Michels, J.; Millard, C.; Singh, J. (2017), supra note 21, pp. 17-18.

applications, such as Bitcoin and Ethereum, they are not suitable for many other economic activities and industries, where efficiency, confidentiality and control over the blockchain are required.[60] In such cases, and whereas a certain level of trust among the participants can be found, blockchain-based platforms do not need to operate in trustless environments and, thus, it is possible to avoid the use of costly consensus mechanisms by relying on trusted intermediaries, such as a single trusted third party or a defined number of nodes.[61]

As private and permissioned blockchains are fully controlled by a single third party (or by a group of nodes that come from a single party), they are often regarded as being completely centralized and closed. Indeed, although private and permissioned blockchain can be designed as open at the user level, meaning that anyone can propose new data to be added to the database, only the trusted third party can perform the role of nodes and miners, *i.e.* to store the copies of the database, and propose and add new blocks to the chain.[62]

As the private and permissioned blockchains allow a single entity to have a *de facto* control over the entire blockchain, these platforms have been explored for the use of both financial and non-financial actors. [63] During the last years, an increasing number of governments around the world have been engaged with blockchain technology, and some of its key uses across the public sector often includes: identity management (proof of identity); government records, which comprises personal records, land registration, and corporate registration; government activities such as electronic voting and tax records; and other similar health and social services.[64] Although private blockchain applications are more efficient, as they operate with a single validator, it must be observed that, due its limited number of participants, these types of blockchains can impose a higher risk to the integrity of data items when compared with public blockchains.[65]

---

60 *See* Bashir, I., (2017), supra note 33, p. 632.

61 S*ee* Bacon, J.; Michels, J.; Millard, C.; Singh, J. (2017), supra note 21, p.19.

62 As an example, considering the use of blockchain technology for land registry purposes, the private and permissioned blockchain models allow any natural or legal person to propose the registry of their land on the database, but only a trusted third party, such as a government agency, can store the registry and add new data to it. In this sense, this trusted third party acts simultaneously as a node and a miner, having a *de facto* power and control over the blockchain.

63 *See* Crosby, M., Nachiappan, Pattanayak, P., Verma, S., and Kalyanaraman, V., (2016), supra note 12, pp. 13-14.

64 *See* Woods, Jorden (2019), "*Blockchain Revolution in the Power Sector*", https://www.blockchainbeach.com/blockchain-revolution-in-the-power-sector-part-1/ [accessed 19 August 2019]. *See also*, *See* Sater, Stan (2017), supra note 14, p. 38.

65 *See* Zheng, Z., Xie, S., Dai, H.N., Chen, X. and Wang, H., (2017), "*An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*". *In* 2017 IEEE International Congress on Big Data (BigData Congress), p. 559.

2.2.3 Consortium blockchains

The consortium blockchains also operate within an environment where a certain level of trust among the participants can be found, but contrary to the private blockchains, instead of relying on a single trusted third entity, the consortium blockchain applications are structured around a defined number of nodes, called '*trusted nodes*'.[66] The consortium blockchains restrict control over the blockchain by giving the possibility to store a copy of the database and to add new blocks on the chain to only a small group of trusted nodes.[67] This signifies that, on the nodes and the miners' level, the consortium blockchains are commonly considered as closed and permissioned platforms. Even at the user's level, it is frequently observed that only authorized parties can join the network. That is case of the R3 Corda, one of the best-known examples of a consortium blockchain platform, which enables a consortium of more than 300 participants of the financial industry '*to transact directly and in strict privacy using smart contracts, reducing transaction and record-keeping costs and streamlining business operations*'.[68] Hyperledger, an open source and modular platform that allows customization and utilizes permissioned blockchain technology to build private business networks, is also another great example of a consortium blockchain platform.[69]

Besides limiting the participation in the network only to a small number of trusted nodes, another characteristic of consortium blockchains, which distinguishes them from both public and private blockchains, lies on its consensus mechanism. As we analyze above, public blockchains uses the PoW protocol to achieve consensus among the nodes and, on private blockchains, there is only a single entity that controls the entire blockchain. Differently, on consortium blockchain, only a small number of nodes participate in the consensus mechanism, which means that an absolute consensus must be achieved in order to add new blocks to the chain. The public blockchain consensus protocols are not adequate for consortium models, as they are costly and require higher amounts of energy and computational power. Thus, instead of relying on asynchronous consensus protocols, consortium blockchains applications typically rely on a traditional and synchronous consensus mechanism.[70] Similar to the private

66 Sometimes, consortium blockchains are designated as '*combined blockchains*'. *See* Fabiano, N. (2018), supra note 13, p. 49.
67 *See* Zheng, Z., Xie, S., Dai, H.N., Chen, X. and Wang, H., (2017 supra note 65, p. 559.
68 *See* https://www.r3.com/platform/ [accessed 19 August 2019].
69 *See* https://www.hyperledger.org/about [accessed 19 August 2019].
70 Synchronous consensus mechanisms are consensus protocols that keep all the nodes in the network synchronized with each other by imposing two requirements: firstly, all the nodes must have an updated copy of the database before moving to the next block; and secondly, before adding a new block to the chain all nodes must achieve consensus. By contrast, asynchronous consensus mechanisms, as the name indicates, do not synchronize

blockchains, the consortium blockchains also present a higher risk to the integrity of data and to the database itself, as the nodes consortium represent single points of failure, which makes them more vulnerable to denial of services attacks and other hacking attacks.[71]

2.3 Blockchain's control and governance

Who controls the blockchain platform? Who can change the platform's design and to what extent? These questions are important not only to conclude our introduction to the blockchain technology, but they are also crucial, as we will see in the following sections, to determine who can be regarded as a controller and/or a processor in the GDPR's perspective.

Each blockchain platform has its own governance rules and its own design and structure. Developers are responsible for producing the software which is used by nodes and miners to support the blockchain.[72] However, the way developers change the platforms' design by introducing changes to the application software can differ substantially, taking into count how platforms were designed in the fist place. For instance, some public blockchain platforms, such as Bitcoin and Ethereum, were developed using an open-source code, which could be used by other developers, rather than the core developers, to write a new version of the software and make it available for the P2P network participants. Typically, apart from the bug fixes, the changes introduced to the blockchain software are meant to achieve other functionalities or to modify the software's capability. Once introduced to the P2P network, nodes and miners can decide which software version they want to run. In case a developer successfully convinced miners and nodes to adopt a new version of the software, a hard fork on the blockchain will be created, originating two different blockchains, in which new blocks will be added subsequently. In the Bitcoin context, when a new version of the software is adopted by nodes

---

with the other nodes, which means that nodes in a network can move to the next block without waiting for an update copy of the database.

71 As the authors Jean Bacon *et al*. state, considering the characteristics of consortium blockchains platforms, it is accurate to see these platforms as a '*permissioned, 'narrowly distributed' platform with a 'shared' (as opposed to distributed) ledger*'. *See* Bacon, J.; Michels, J.; Millard, C.; Singh, J. (2017), supra note 21, p. 21.

72 In the Bitcoin context, it is possible to split the developers' group in two other groups: the developers' group, who can propose new technical improvements; and the core developers' group, who has the power to introduce changes to the Bitcoin Core software. *Ibid*. *See* also Vetter, Greg R., (2004) ''Infectious' Open Source Software: Spreading Incentives or Promoting Resistance?', Rutgers Law Journal, University of Houston Law Center, No. 2004-A-11, pp. 77-88.

and miners a hard fork is created, giving rise to new blockchains, one that continues to track bitcoins, and a new one that now tracks a new crypto coin.[73]

On the contrary, on private and consortium blockchains, new versions of the software that supports the blockchain can be subjected to contractual provisions that were negotiated between the parties involved in the creation and development of a particular blockchain platform. In such cases, it can be argued that the developers' role is limited to the performance of contractual obligations, as they do not typically have the power or the means to change the software version by their own initiative.

Finally, there is a fifth intervenient group on the blockchain environment: the service providers. Normally, service providers intervein on blockchain platforms either by offering services related to online wallets or by offering '*Blockchain-as-a-Service*'.

Online wallets are digital wallets that work as an interface to a blockchain system, allowing users to manage crypto coins or other digital assets. When using an online wallet, the users are provided with a wallet ID, which is a unique identifier such as a bank account number. However, this wallet ID is completely different from the private and public key pair, which is generated by those services on the users' behalf.[74]

On other hand, '*Blockchain-as-a-Service*' is a service that allows the customer to leverage cloud-based solutions to create their own blockchain applications. The service providers' offer includes a wide range of task and activities that can include the management of the platform, the hosting of a certain number of nodes, or even the management of identity authentication. Since the service providers have a direct involvement on the blockchain platform creation and control, this might raise some questions related to the degree of power and the control the service providers have over the blockchain. As we will analyze below, these questions are important to determine the nature of service providers in the context of the GDPR, namely, to assess whether the service providers can determine the purposes and the means of the processing of personal data.

---

73 Currently, there are 105 Bitcoin forks of which 74 are considered active projects, and 34 are regarded as historic projects. For an overview of all Bitcoin forks, *see* https://forkdrop.io/how-many-bitcoin-forks-are-there [accessed 19 August 2019].

74 When using an online wallet, users must bear in mind that relying on an intermediary could jeopardize the security of their assets, as those service providers are not immune to cyberattacks and other risks that could result in the lost of the users' private and public key pair. Actually, phishing attacks are often directed against online wallets. *See* Khatri, Yogita, (December 28, 2018) "*Electrum Wallet Attack May Have Stolen As Much as 245 Bitcoin*" *in* https://www.coindesk.com/electrum-wallet-attack-may-have-stolen-as-much-as-245-bitcoin [accessed 19 August 2019].

3. IDENTITY OF THE BLOCKCHAIN PARTICIPANTS

As previously stated, the taxonomy (*i.e.* the structure, organic, etc.) of the blockchain applications has a different impact on the powers, rights, permissions and restrictions of the participants of a particular platform. Typically, any participant, or even the public, can consult the entire blockchain archive of a public and permissionless blockchain application. By contrast, on consortium blockchain applications, the archives' reading permissions can be limited to a certain number of participants, while on private and permissioned blockchain applications, the access to the blockchain archives can be denied or limited to a few blocks or certain data entries.[75]

This immediately raises two mains questions: can participants of the blockchain platforms be identified? If so, can any other participant access their data and transactions' history?

As stated above, blockchain applications use a PKI to authenticate the identity of their participants. In general, the public and private key do not reveal the participants real-world identify. Early blockchain applications, such as Bitcoin, took these concerns into account and, as Nakamoto (2009) explains: '*privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone*'.[76] Additionally, users can generate a new private and public key pair for each new transaction.[77] This level of pseudonymization ensures that even on public blockchains, where anyone can consult the blockchain archive, no one will be able to determine the real-world identity of the parties involved in a particular transaction.

However, the users' identity can be exposed on a voluntary basis, if the users decide to reveal their real-world identity, or on an involuntary basis, as it is the case of malicious attacks on online wallets, in which the attacker has obtained access to user information. In the same way, the real-world identity of a user can be indirectly revealed by linking different data elements. For instance, if a user uses bitcoin as a method of payment to buy goods or services, the other party might need the customer's name, email address, postal address, and other

75 *See* Zheng, Z., Xie, S., Dai, H.N., Chen, X. and Wang, H., (2017 supra note 65, p. 559
76 *See* Nakamoto, Satoshi, (2008), supra note 3, p. 9.
77 *Ibid*.

personal information that can lead to the identification of the user.[78] The IP addresses can also be used as a way to determine the users' identity by linking the users' private and public key pair to the locality from which the transaction was generated.[79]

Although the PKI ensures a certain level of protection to the users' identity, once their real-world identity has been revealed, anyone can access the entire transaction history associated with that user, especially in cases where the private and public key pair has not been changed. Although private and consortium blockchains normally operate in an environment where trust among participants can be found, and where sometimes the participants know each other, these blockchain types can limit the access level to the blockchain archive, ensuring that the users' identity remains properly protected.

78 *See* Reid, F. and Harrigan, M., (2013), "*An analysis of anonymity in the bitcoin system*", Security and privacy in social networks, Springer, New York, p. 15, *apud* Bacon, J.; Michels, J.; Millard, C.; Singh, J. (2017), supra note 21, p. 27.

79 *See* Biryukov, A., Khovratovich, D. and Pustogarov, I., (2014), "*Deanonymization of clients in Bitcoin P2P network*" *in* Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (pp. 15-29), *apud* Bacon, J.; Michels, J.; Millard, C.; Singh, J. (2017), supra note 21, p. 27.

4.LEGAL TENSIONS BETWEEN BLOCKCHAIN TECHNOLOGY AND THE GDPR

The European Union's General Data Protection Regulation (GDPR) entered into force in May 2016 and became legally binding in May 2018, replacing the 1995 Data Protection Directive.[80] The GDPR establishes a homogenous legislative framework across the European Union, ensuring a high-level protection of natural persons and the removal of the obstacles to flows of personal data between all the Member States.[81]

The GDPR is an innovate legal framework that changed how data protection is perceived and how the processing of personal data should be regulated by the law.[82] By introducing new data protection rights and obligations, and enforcing a *'data protection by design'* approach, the reform of the European Union's legal framework on data protection has influenced the usage and development of new technologies such as blockchain. In this context, a common critique emerges among the data protection authors, who affirm that the European legislator has failed to take into proper consideration the emergence of new technologies, especially technologies that were under development when the GDPR draft was elaborated.

In fact, several tensions between GDPR and blockchain have been identified, revealing the difficulty GDPR has in keeping pace with blockchain technology.[83] Without prejudice to other factors, the tensions between GDPR and blockchain technology occur at two mains levels: firstly, the GDPR implicitly assumes that data is controlled or processed by identifiable actors;[84] and secondly, it also assumes that the data subjects' personal data can be rectified or erased in any case, to comply with the legal requirements set under articles 16 and 17 of the GDPR.[85]

In this section, after analyzing the GDPR territorial and material scope, and defining what is considered personal data in the context of blockchain technology, we will examine the legal tensions between the blockchain and the GDPR in further detail.

---

80 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) *in* Official Journal of the European Union, L 119/1, 4.5.2016, pp. 1-88.

81 Article 1(1) and Recital 10 of the GDPR.

82 *See* Giannopoulou, Alexandra and Ferrari, Valeria, (2016), "Distributed Data Protection and Liability on Blockchains", in Internet Science: 5th International Conference proceedings, Vol. 2. Workshops; Amsterdam Law School Research Paper No. 2019-06; Institute for Information Law Research Paper No. 2019-03. p 204.

83 *See* Finck, Michèle (2019), supra note 19, p. II.

84 *See* Lyons, T., Courcelas, L., and Timsit, K. (2018), supra note 51, p. 17.

85 *See* Finck, Michèle (2019), supra note 19, p. II.

4.1 The GDPR's applicability to blockchain-based platforms

Taking into account the objective of ensuring a consistent and homogenous protection of the natural persons with regard to the processing of their personal data, the GDPR's material and territorial scope is broad, covering a wide range of cases that also include the data processing activities taking place outside of the European Union territory.

With respect to its territorial scope, the article 3 (1) of the GDPR states that the regulation applies to all data controllers and processors established in the European Union, regardless of whether the processing takes place in the Union or not. The recital 22 of the GDPR clarifies that establishment of a controller or processor '*implies the effective and real exercise of activity through stable arrangements*', which suggests that the concept of establishment is not limited to its formal elements but, on the contrary, includes its functional elements as well.[86] In line with this approach is the case law of the European Court of Justice (ECJ), who in the *Weltimmo* case explained that '*the degree of stability of the arrangements and the effective exercise of activities (…) must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned*'.[87] In the *Google Spain* case, the ECJ also stated that the '*the European Union legislature sought to prevent individuals from being deprived of the protection guaranteed by the directive and that protection from being circumvented, by prescribing a particularly broad territorial scope*'.[88] Thus, due to the flexible concept of '*establishment*', it is likely the territorial scope of GDPR will be fulfilled for most part of the blockchain operators established within the Union, unless the household exception under the article 2 (2) (c) of the GDPR applies.

In case the establishment criterion does not trigger the GDPR's application, the article 2 (a) and (b) of the GDPR extends its territorial scope to data controllers and processors not established in the Union, where the processing activities relates to the offering of goods or services to the data subjects who are in the Union,[89] and to the monitoring of the data subjects behavior, as far as their behavior takes place within the Union.

Due to its broad territorial scope, the GDPR is most likely to apply to a wide range of blockchain-based platforms and its operators. For instance, the GDPR will be applicable in relation to all blockchain operators who are established outside of the Union territory,

86 *See* Finck, Michèle (2019), supra note 19, p. 8.
87 *See* Case C-230/14, Weltimmo, EU:C:2015:639, 1 October 2015, para. 29.
88 *See* Case C-131/12, Google Spain, ECLI:EU:C:2014:317, 13 May 2014, para.
89 The reference of to the data subjects '*who are in the Union*' set under the article 3 (2) of the GDPR is related to the data subjects' location, not their nationality.

whenever they offer services to data subjects who are in the Union. In the same way, the operators of open and permissionless blockchain-based platforms are also subjected to comply with the GDPR rules, as it could be argued that those types of platforms offer services to data subjects who are in the Union. This is the case of Bitcoin, a platform that offers an electronic payment method to data subjects in the Union.[90]

Under the article 2 (1) of the GDPR, the regulation applies to the processing of personal data wholly or partly by automated means as well as personal data processing that relies on non-automated means, but forms part of, or is intended to form part of, a filling system. According to article 4 (2) of the GDPR, personal data processing is '*any operation or set of operation which is performed on personal data or on sets of personal data, whether or not by automated means*'. The general definition of '*processing*' includes the '*collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*' of personal data. However, under its case law, in particular under the *Bodil Lindqvist* case, the ECJ noticed that these are mere examples of personal data processing, as the concept of '*processing'* is meant to be interpreted broadly.[91]

In this context, one can argue that the main functions of blockchain-based platforms are precisely to transmit, store and record personal data by automated means. For such reason, it could be said that blockchain participants are undoubtedly engaged in the processing of personal data, which, considering its material scope, triggers the GDPR's application, unless the household exception set under the article 2 (2) (c) of the GDPR is applicable. [92]

4.2 Personal Data on Blockchain

In accordance with recital 26 of the GDPR, *the principles of data protection should only apply to any information concerning an identified or identifiable natural person*, which

90 As we will analyze under the section 4.3 of your study, determining the data controllers and processors of a public and permissionless blockchain-based platform is not straightforward. In the context of the territorial scope of the GDPR, Bacon *et al.* suggest that nodes and miners are operators of the Bitcoin platform, as they support it collectively, and thus they are obligated to comply with the GDPR rules. Although we agree with the authors, it becomes clear that it is extremely difficult to identify them individually, which jeopardizes the GDPR's level of protection regarding the processing of personal data. *See* Bacon, J.; Michels, J.; Millard, C.; Singh, J. (2017), supra note 21, p. 39.

91 *See* Case C-101/01, Bodil Lindqvist, EU:C:2003:596, 6 November 2003, para. 25.

92 *See* Giannopoulou, Alexandra and Ferrari, Valeria, (2016), supra note 82, p. 205.

signifies that GDPR's applicability to the blockchain-based applications and their operators is, in any case, dependent on the qualification of the data stored and processed in the blockchain as personal data.

The article 4 (1) of the GDPR incorporates a wide definition of 'personal data'. It includes any information that directly or indirectly relates with an identified or identifiable natural person. In order to determine whether a natural person is identifiable, recital 26 of the GDPR, states that *all the means reasonably likely to be used (…) to identify the natural person directly or indirectly* should be taken into consideration. To ascertain what are the reasonable means likely to be used, objective factors should be taken into consideration. Recital 26 of the GDPR highlights some of those factors, which include: *i)* the costs of and the amount of time required for identification; *ii)* the technology that is available at the time of processing; and *iii)* the technological developments. The ECJ case law also reflects the broad interpretation of '*personal data'*. For instance, in the *Digital Rights Ireland* case, the ECJ has determined that the definition of 'personal data' is broad enough to qualify the metadata (*e.g.* the location of mobile communication equipment, IP address, *etc*.) as personal data, as the usage of this type of data makes it possible to identify a person, and it '*may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained*'.[93]

The online identifiers provided by the data subjects' devices, applications, tools and protocols, can also be used to directly or indirectly identify them. As the recital 30 of the GDPR recognizes, the online identifiers *'may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them*'.

The broad definition of personal data also includes the personal data which have undergone pseudonymization. Contrary to anonymization, the application of pseudonymization to personal data is deemed as a security measure that contributes to mitigate the risks to the data subjects in relation to the processing of personal data.[94] In fact, the Article 29 Working Party (hereafter WP29) expressly recognizes that '*pseudonymization is not a method of anonymization. It merely reduces the linkability of a dataset with the original identity of a data subject, and is accordingly a useful security measure*'.[95] In this sense, the usage of encrypted and hashed techniques to store and process data on blockchain-based applications

93 *See* Cases C-293/12 and C-594/12, Digital Rights Ireland, EU:C:2014:238, 8 April 2014, para. 26 and 27.
94 Recital 28 and Article 32 (1) (a) of the GDPR.
95 *See* Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (WP 216) 0829/14/EN, p. 3.

are deemed to be qualified as a particular method of pseudonymization, considering that an important factor to qualify data as being anonymous is that the processing of re-identification of a natural person must be irreversible.[96] Bearing in mind the broad definition of personal data, blockchain-based applications are likely to process, at least, two types of personal data: public keys and transaction data.[97]

As previously explained, on blockchain-based applications, public keys are used essentially for identification purposes, while private keys are mostly used for authentication and encryption purposes. The private and public key pair, represented by a string of letters and numbers, is used to hide the real identity of the natural persons. As the WP29 sustains, the '*pseudonymisation is the process of disguising identities. The aim of such a process is to be able to collect additional data relating to the same individual without having to know his identity*'.[98] In this regard, and taking into consideration the provisions set under the article 4 (5) of the GDPR, it could be argued that the private and public key pair is likely to be qualified as a pseudonymization method, as the identity and other personal data can no longer be attributed to a specific data subject without using additional information. As the WP29 expressly recognizes, using a pseudonym means that it is still possible, under certain circumstances, to backtrack the individuals and discover their identities.[99]

Indeed, there are some practices and methods to determine the identify of the holders of a private and public key pair. Besides the voluntary disclosure of the private and public key pair, it is possible to identify a natural person when additional information is gathered in accordance with other regulatory requirements – as it is the example of the Anti-Money Laundering duties – and then, combined with that, the specific private and public key pair.[100] On Bitcoin's platform, it is also possible to determine the identity of a data subject by linking its public key to its IP address.[101] The pattern of transactions can also be used to single out a particular data subject by using the 'transaction graph analysis' technique, which allows the

96 As the WP29 acknowledges, '*anonymisation is increasingly difficult to achieve with the advance of modern computer technology and the ubiquitous availability of information. Full anonymisation would also require, for instance, that any reasonable possibility of establishing a link with data from other sources with a view to re-identification be excluded*.' *See* Article 29 Working Party, Opinion 03/2013 on purpose limitation (WP 203) 00569/13/EN, p. 31.

97 *See* also Edgar, Laura, (2018), "*Blockchain and data protection: evaluating the legal compatibility of blockchain technology with the general data protection regulation*", Queen Mary University of London, Centre of Commercial Law Studies, p. 39.

98 *See* Article 29 Working Party, Opinion 04/2007 on the concept of personal data (WP 136) 01248/07/EN, p. 18.

99 *Ibid.*

100 *See* Finck, Michèle (2019), supra note 19, p. 27.

101 *See* Bacon, J.; Michels, J.; Millard, C.; Singh, J. (2017), supra note 21, p. 40.

determination of the identity of a certain unknown user by analyzing her transactional activity with a known user of a certain blockchain-based application.[102] In this context, one can argue that the private and public key pair should be regarded as person data in the terms of the article 4 (1) of the GDPR, since it could potentially lead to the direct or indirect identification of a natural person.

In many circumstances, the object of transactions – or the transactional data – can also be regarded as a personal data, as this type data can be linked to a real-world identity. Aside for the private and public key pair, the transactional data includes all the other categories of data that a transaction can contain. For instance, if a group of banks uses a consortium blockchain-based application to share Know Your Client information, the data contained in those transactions are deemed to be qualified as personal data, since such data concerns identified or identifiable natural persons. The transactional data can be used in plain text, in an encrypted form, or it can be hashed.

When transactional data is used in plain text, containing any information relating to an identified or identifiable natural person, there is no doubt concerning its qualification as a personal data.

As for encryption, as the WP29 correctly describes, it is one of the most used pseudonymization techniques.[103] As stated above, although this technique contributes to reduce the linkability of a particular dataset with the identify of a data subject, it is a useful security measure, but it cannot be considered an anonymization method.[104] Indeed, the holder of the private and public key pair can still be re-identified through the decryption processes. In this context, one can argue that personal data is still storage in a dataset that has been encrypted and, thus, encrypted data should be qualified as personal data.[105]

Contrary to the use of encryption techniques, hash functions cannot be reversed, which means that once data has been put through a hash algorithm – such as the SHA-256 – that has transformed the input value into an output value with a fixed length, the hash function cannot run backward. Nevertheless, this does not automatically mean that hash functions are a method of anonymization,[106] as the linkability between a particular dataset and the hash function's

---

102 *Ibid.*
103 *See* Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (WP 216) 0829/14/EN, p. 20.
104 *Ibid*.
105 *See* Finck, Michèle (2019), supra note 19, p. 29.
106 As the WP29 states, the use of a (salted) hash function '*can reduce the likelihood of deriving the input value but nevertheless, calculating the original attribute value hidden behind the result of a salted hash function may*

output value can still be found. As the WP29 corroborates, in case the range of an input value is known, it can be replayed through a hash function, in order to achieve the accurate value of a particular dataset.[107] To Michèle Finck, a non-invertible hash function must ensure that the possible inputs are sufficiently large and unpredictable to prevent the option of trying all the possible combinations, but as the author recognizes, this is hard to achieve, especially if we are to consider the increasing power and decreasing cost of computing.[108] Therefore, following the WP29's opinion, hashing will generate pseudonymized data in most cases, even where hash functions with stronger privacy guarantees are used (*e.g.* salted hash, peppered hashes, keyed-hash functions with stored key, keyed-hash functions with deletion of the key, etc.).[109]

Without prejudice to a case-by-case analysis, it could be argued that encryption and hash functions are specific methods of pseudonymization that do not preclude the GDPR's applicability, considering the recital 26 test and the article 4 (1) and (5) of the GDPR.

4.3 Allocating responsibilities within blockchain platforms

Enhancing the protection of natural persons with regards to the processing of personal data is one of the two main objectives of the GDPR[110] and, for such reason, the accountability principle set under the article 5 (2) of the GDPR (which extends to processors) obliges controllers to take responsibility and demonstrate compliance with all the other principles set under the same article. Indeed, controllers are obligated to implement appropriate technical and organizational measures in order to demonstrate that its data processing is performed in accordance with the GDPR.[111] When contracting with a processor to process personal data on the controller's behalf, the later shall also use processors who have provided sufficient

still be feasible with reasonable means.' *See* Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (WP 216) 0829/14/EN, p. 20.

107 The WP29 provides the following example: '*if a dataset was pseudonymised by hashing the national identification number, then this can be derived simply by hashing all possible input values and comparing the result with those values in the dataset*'. *Ibid*.

108 *See* Finck, Michèle (2019), supra note 19, p. 30.

109 *See* Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (WP 216) 0829/14/EN, p. 20.

110 Article 1 (1) of the GDPR.

111 Article 24 (1) of the GDPR.

guarantees that technical and organizational measures were implemented in accordance with the GDPR.[112]

The GDPR's structure defines the roles of controllers and processors in a clear and objective fashion, which is well adapted to scenarios where it is possible to find a central entity responsible for processing personal data, but remains inadequate to all the scenarios in which data is being processed in a distributed way.[113]

According to the article 4 (7) GDPR, the controller is any natural or legal person, which alone or jointly with others, determines the purpose and means of the processing of personal data. In the WP29's opinion, '*determining the purposes and means amounts to determining respectively the 'why' and the 'how' of certain processing activities*'.[114] The WP29 also clarifies that '*The concept of controller is a functional concept, intended to* ***allocate responsibilities where the factual influence is****, and thus based on a factual rather than a formal analysis*'.[115] Although the two elements, '*means'* and '*purposes*', appear to have an equivalent importance to determine who the controller is, in the WP29's opinion, the purposes criterion has primacy over the means criterion, as the '*determination of the "purpose" of processing is reserved to the "controller"*' and the '*determination of the "means" of processing can be delegated by the controller, as far as technical or organisational questions are concerned*'.[116] Aligned with this view, in the *Google Spain* case the ECJ also stated that, in order to ensure an effective and complete protection of data subjects, the concept of '*controller*' should be interpreted broadly.[117]

Finally, according to the article 4 (8) of the GDPR, the processor is any natural or legal person who processes personal data on behalf of the controller. The existence of a processor depends on the controller's decision, who might decide to delegate all or part of the processing activities to another natural or legal person. Therefore, two basic conditions must be present to qualify any person or entity as a processor: firstly, the processor must be a separate legal entity

112 Article 28 of the GDPR.
113 *See* Ibáñez, Luis-Daniel, O'Hara, Kieron and Simperl, Elena (2018), supra note 4, p. 5.
114 *See* Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169) 00264/10/EN, p. 13.
115 *Ibid.* (our own emphasis).
116 *Ibid*., p. 15.
117 *See* ECJ, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C‑131/12, 13 May 2014, para. 34.

with respect to the controller; and secondly, the processing activities are conducted by that separate legal entity on the controller's behalf.[118]

As we will see below, identifying a controller or a processor in blockchain-based applications is not straightforward. In order to answer the question '*Who determines the purposes and means of data processing?*', it is not only necessary to consider the specificities of each case and the manner in which personal data is being processed, but also to examine the structure and governance design of the different blockchain platforms. Thus, considering the criterion provided by the WP29 and the relevant ECJ case-law, we analyze next the possible qualification of blockchain actors across the different blockchain types.

4.3.1 Allocating responsibilities within public blockchains

As mentioned under the section 2.2 of our study, there are three main actors on blockchain: the users, who propose new transactions; the nodes, who store copies of the distributed database; and the miners, who propose new blocks by executing a consensus protocol. Apart from these actors, we also have the developers, who produce the software which is used by nodes and miners to support the blockchain, and the wallet providers, who generate a private and public key pair on the users' behalf, providing them with a service that works as an interface to a specific blockchain platform, from which they can manage crypto coins or other digital assets. As we also explained before, open and permissionless blockchain-based platforms lack a central administrator, since the control over the platform is intentionally distributed. For this reason, determining who are the controllers and the processors has been a difficult exercise, as the definitions set under the article 4 (7) and (8) of the GDPR are ill-suited to these types of platforms.[119] Additionally, there is not a common understanding on the literature on DLTs and GDPR about which actor should be regarded as being the controller. [120]

The difficulty to determine who is a controller in an open and permissionless blockchain platform arises from two main factors: firstly, there is a wide number of the actors that influence the means of processing personal data; and secondly, the purposes of processing personal data are also fragmented.[121]

---

118 *See* Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169) 00264/10/EN, p. 25.
119 *See* Bacon, J.; Michels, J.; Millard, C.; Singh, J. (2017), supra note 21, p. 43.
120 *See* Finck, Michèle (2019), supra note 19, p. 43.
121 *Ibid*.

To surpass these difficulties, Bacon *et al*. sustain that determining who is the controller requires an analysis that should be based on a micro-level perspective (*i.e.* the individual transactions), where '*the choice of the blockchain platform*' is the decisive criterion.[122] Thus, the macro-level perspective, which determines the controller by taking into account the blockchain infrastructure as a whole (*i.e.* as a service) should be rejected. In our view, this position should be adopted alongside with the criterion extracted from the WP29's guidelines and the ECJ case-law. Indeed, the DLTs are a mere infrastructure where blockchain applications, its design and governance structure can be developed and, since the processing of a specific item of personal data is more relevant to the GDPR, the micro-level perspective is more adequate to determine which actor can be considered a controller.

In this context, and without prejudice of a case-by-case analysis, it could be argued that when deciding to use an open and permissionless blockchain platform (*e.g.* Bitcoin) for a specific purpose (*e.g.* to make a transaction), the users determine the '*purposes*' and '*means*'. In such case, the user has opted for using the Bitcoin blockchain (the *'means*') to make a transaction (the '*purpose*'), when she arguably had the option to choose a different type of payment and another platform to make the transaction. Unless the user is a natural person that is using Bitcoin blockchain in the course of a purely personal or household activity, as defined under the article 2 (1) (c) of the GDPR, she should be considered a data controller.[123]

In this regard, although nodes and miners exercise significant control over the means (*e.g.* Bitcoin blockchain) by choosing to run a specific software and its embedded protocols, they usually do not determine the purposes, which is, as we analyze above, the main criterion to determine who is the controller. [124] Therefore, generally speaking, the nodes and miners are considered to be data processors. [125] However, it must be acknowledged that, in certain cases, nodes and miners can define their own purposes and set up their own means. For instance, these actors can access the public database stored on the blockchain to collect personal data for commercial purposes, or they can also change the rules of the blockchain-based platforms by

122 *See* Bacon, J.; Michels, J.; Millard, C.; Singh, J. (2017), supra note 21, pp. 41-45.
123 *Ibid*. *See* also Finck, Michèle (2019), supra note 19, pp.46-47; Giannopoulou, Alexandra and Ferrari, Valeria, (2016), supra note 82, pp. 208-210.
124 *See* Finck, Michèle (2019), supra note 19, p. 47.
125 In its guidance, the French supervisory authority (Commission Nationale Informatique et Libertés) considers that '*The miners limit themselves to the validation of the transactions submitted by the participants and do not intervene on the object of these transactions: they do not determine how the finalities and the means will be implemented'*. *See* Commission Nationale Informatique et Libertés, 'Premiers Éléments d'analyse de la CNIL: Blockchain' (September 2018), p. 2 (translated).

creating a fork in the chain. In such cases, nodes and miners became joint controllers in the meaning of article 26 of the GDPR.

4.3.2 Allocating responsibilities within private blockchains

Contrary to public and permissionless blockchain-based platforms, closed and permissioned blockchain-based platforms are usually controlled by a centralized entity (*e.g.* a company, a public agency, etc.), who not only controls the means, but in many cases also determines the purposes of the processing of personal data. In such cases, authors like Michèle Finck tend to qualify the platform operator as a data controller, since the means and purposes of the processing are essentially determined by such entity.[126]

By contrast, authors like Jean Bacon *et al*. consider that such a conclusion is only possible from a macro-level perspective, which focuses on the blockchain infrastructure as a whole. However, taking into account the micro-level perspective,that focuses on individual transactions, these authors consider that users should be considered data controllers, whereas the centralized entities only act as a data processor.[127] Using the example of a land registry, this conclusion is supported by the idea that users insert personal data onto private and permissioned blockchain-based platforms for their own purposes (*i.e.* register or transfer titles of land) and, since they also chose those platforms as a medium to execute their transfers, they also determine the means of processing.[128]

With due respect to both positions, and without prejudice to a more detailed case-by-case analysis, we sustain that the identification of a data controller should take into account the criterion defined by the Article 29 Working Party (WP29), in which the allocation of responsibilities should be based on where the factual influence could be found.[129] In this sense, if the users have limited choice regarding the platform, it is not feasible to sustain that they have a factual influence over the purposes and means of the processing. For instance, if a government agency implements a land registry blockchain-based platform, compelling the citizens to adopt it when registering and transferring titles of land, the users do not exercise

126 *See* Finck, Michèle (2019), supra note 19, p. 44. *See* also Giannopoulou, Alexandra and Ferrari, Valeria, (2016), supra note 82, p. 208; and, Ibáñez, Luis-Daniel, O'Hara, Kieron and Simperl, Elena (2018), supra note 4, p. 5.
127 *See* Bacon, J.; Michels, J.; Millard, C.; Singh, J. (2017), supra note 21, p.42
128 *Ibid*.
129 *See* Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169) 00264/10/EN, p. 9.

any factual influence over the means and the purposes of the processing. One could argue that, in any case, the users decide to continue using the land registry platform for their own purposes. However, in cases such as this, their decision is greatly influenced by the government agency and, thus, the users' decision is limited *ab initio*. On another hand, if the users decide to use a closed and permissioned blockchain-based platform, where they could have chosen another means, they should be considered data controllers, since they truly determine the purposes (*e.g.* transfer a digital asset to other person) and means (*e.g.* using Blockchain-as-a-Service). In a case like this, the entities offering Blockchain-as-a-Service should be considered a data processor, unless they use the personal data for their own purposes.

4.3.3 Allocating responsibilities within consortium blockchains

As we previously observed, consortium blockchains are a permissioned, narrowly distributed platform, controlled by a small number of trusted nodes. The R3 Corda is one of the best-known consortiums blockchain-based platforms, where more than 300 financial entities participate by sharing information and settling payments among themselves. There are also other consortium blockchain-based applications in which banks and other financial institutions share information about their clients in order to comply with Know Your Client (KYC) and Anti-Money Laundering (AML) laws. These types of platforms are commonly designed as closed and permissioned, as only authorized participants can use the platforms and access the blockchain database.[130]

Similar to the private blockchain-based platforms, on consortium blockchains, the participating nodes act as a centralized entity, exercising a factual influence on the platform by determining the means and the purposes of the processing. In this sense, at the users' level, the participating nodes should be regarded as data controllers. Indeed, in such cases, it must be observed that the financial entities choose to use a certain mean (*e.g.* to use R3 Corda and similar platforms) to submit data about their clients and use the data on the blockchain database for their own purposes (*e.g.* to comply with AML and KYC laws). Regarding the other participants of a consortium blockchain-based platform, who process personal data as nodes and miners, they should be considered data processors, unless they use the personal data that is stored on the database for their own purposes, in which case they should be qualified as data controllers.

130 *See* Bacon, J.; Michels, J.; Millard, C.; Singh, J. (2017), supra note 21, p. 43.

4.4 Data Subjects Rights

The allocation of responsibilities within a certain blockchain-based application is of crucial importance not only to comply with the GDPR's technical and organizational requirements, but also to allow data subjects to exercise their rights. The articles 15 to 22 of the GDPR incorporate specific rights of the data subjects, among which there are the right of access (article 15), right to rectification (article 16) and right to erasure (article 17). As we analyze below, blockchain-based applications, especially the open and permissionless blockchains, impose serious limitations to the exercise of some of the data subject's rights and freedoms, as the immutability feature of those applications is hard to combine with the desirable flexibility of a database, which seems necessary to comply with the data subjects' requests.

In accordance with the article 15 (1) of the GDPR, the data subject has the '*right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed'*, and, where that is the case, access the personal data and the information considering, *inter alia*, the purposes of the processing, the categories of personal data, the recipients to whom the personal data have been disclosed, the duration of storage, and the existence of automated decision-making. Under the article 15 (2) of the GDPR, data subjects also have the right to be informed about the adoption of the appropriate safeguards set under the article 46 of the GDPR, with respect to the transfer of personal data to third countries or international organizations. As we will analyze on the next point of our study, transfers of personal data to third countries can create a legal tension between the GDPR and some blockchain-based applications, considering that nodes located in the European Union probably share data with nodes that are located in other jurisdictions, without relying on a legal basis for such transfer.

The data subjects' right of access may be difficult to exercise in a context where personal data is processed on a blockchain-based application, especially on the open and permissionless blockchains. Since blockchain-based applications often rely on the use of encryption techniques and hash functions to pseudonymize personal data, it may be difficult for nodes to know exactly which data is stored on a blockchain database and provide the data subject with information concerning the processing of her personal data.[131] A similar problem arises in

131 *See* Edgar, Laura, (2018), supra note 97, p. 46.

relation to the provision established under the article 15 (3) of the GDPR, which entitles the data subject to receive a copy of her personal data undergoing processing.[132] Taking into consideration the open and permissionless blockchain-based applications, it may be impossible for nodes to provide a copy of the undergoing personal data processing not only because they are in no position to know which data is being processed, but also because they can only provide the data subject with their local copy of the blockchain database, which does not guarantees, *per se*, that is the copy other nodes on the P2P network are using to process data. On the contrary, on closed and permissioned blockchains, data controllers are in better position to facilitate the exercise of the data subjects' rights, as the users and nodes of these type of blockchain-based applications, who are regarded as being the data controller, have more control over the processing of personal data and, in general, over the platform.

The right to rectification, established under the article 16 of the GDPR, provides the data subject with the right to obtain, from the controller, the rectification of inaccurate personal data. The right to rectification is intrinsically related to the accuracy principle set under the article 5 (1) (d) of the GDPR, which determines that '*every reasonable step must be taken to ensure that personal data that are inaccurate (...) are rectified without delay'*.

However, even though data subjects themselves can be qualified as data controllers in many cases, exercising the right to rectification can be extremely challenging, considering the immutability characteristic of blockchain technology. Indeed, exercising the right to rectification on open and permissionless blockchain-based applications is tremendously impractical or almost impossible. First, the nodes only can alter their own local copy of the blockchain database and, as we analyzed before, such modification is irrelevant as nodes and miners tend to use the blockchain database version used by the majority of blockchain's participants.[133] Second, it may be impossible for a data subject to identify all the nodes, or to identify enough nodes (51%) to create a fork on the blockchain, in order to rectify her personal data. Third, even if enough nodes were identified, it would be extremely difficult to ensure such level of coordination.[134] On the other hand, the operators and data controllers of closed and permissioned blockchain-based applications, as it is the case of private and consortium blockchains, are in a better position to comply with the data subject's requests, as the

132 *See* Finck, Michèle (2019), supra note 19, p. 72.
133 *See* point 2.2.1 of our study.
134 *See* Berberich, Matthias and Steiner, Malgorzata (2016), "Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers", 2 Eur. Data Prot. L. Rev. pp. 422-426.

centralized characteristics of these types of blockchains allows for better reversibility than the open and permissionless blockchains.[135]

Under the provisions established under the article 17 (1) of the GDPR, the data subject has '*the right to obtain from the controller the erasure of personal data concerning him or her without undue delay'*. In accordance with article 17 (2) of the GDPR, in case the controller has made the personal data public, as it is often the case of open and permissionless blockchains, the controller, taking into account the available technology and the cost of implementation, shall inform other controllers which are processing the personal data over which the data subject has exercised her rights. Similar to what we examined in relation to the right to rectification, the right of erasure is intrinsically related to the accuracy principle set under the article 5 (1) (d) of the GDPR.

As stated above, the immutable characteristic of blockchain-based applications makes it difficult (or near impossible) to change or delete any data stored into the blockchain database. In this sense, it could be argued that the creation of hard forks inside a blockchain could be a valid option to comply with the data subjects' right to erasure. However, besides the difficulties originated in trying to achieve such level of coordination among the nodes, the creation of hard forks is of a very exceptional nature, and it does not constitute a viable method to ensure the exercise of the right to erasure.[136] Additionally, such option could lead to the inoperability of blockchain-based applications, as hard forks invalidate all the subsequent blocks in the chain, forcing the nodes and miners to re-hash, validate and append all the other valid blocks into the chain, which would require long periods of time and it would be particularly costly in some cases.

In this context, it seems that blockchain-based applications cannot comply with the right to erasure (especially the open and permissionless blockchain-based applications). Nevertheless, it has been argued that the meaning of '*erasure*' is open to interpretation, as it can include, for instance, the simple removal of personal data from a search index and not the personal data itself, as the ECJ ruled, which is regarded as a '*soft version of the right to be forgotten*'.[137] Although we tend to agree that the meaning of '*erasure*' is open to interpretation and the inclusion of the expression '*available technology*', in the article 17 (2) of the GDPR, suggests that blockchain features shall be taken into consideration in relation to the exercise of

135 *See* Bacon, J.; Michels, J.; Millard, C.; Singh, J. (2017), supra note 21, p. 47.
136 *See* Finck, Michèle, (2017), "Blockchains and Data Protection in the European Union", Max Planck Institute for Innovation & Competition Research Paper No. 18-01, p. 31.
137 *Ibid*.

the right to erasure,[138] it seems improbable, at current time, that the design and key features of early blockchain-based applications would comply with the requirements of the article 17 of the GDPR. For the reasons already presented in relation to the right to rectification, private and consortium blockchain-based applications are, in principle, in a better position to comply with the right to erasure.

In accordance with the article 19 of the GDPR, the controller shall communicate any rectification or erasure to every recipient who received a certain data subject's personal data, unless this proves to be impossible or in case it involves a disproportionate effort. Once again, considering the difference between open and permissionless and closed and permissioned blockchain-based applications, the provision of the article abovementioned may not be applicable to the former since it can involve a disproportionate effort or, in some cases, it may be virtually impossible.

Although the majority of the most well-known blockchain-based applications, such as Bitcoin or Ethereum, does not allow data subjects to fully exercise their rights under the GDPR, some solutions have been presented and proposed to surpass those difficulties. As we will analyze next, the off-chain repository solution provides a simple and easy answer to mitigate the legal tensions that occur at the data subjects' rights and freedoms level.

4.5 Personal Data transfer to third countries

In line with articles 44 to 49 of the GDPR, personal data can only be transferred to third countries on the basis of an adequacy decision; if the controller or processor has provided appropriate safeguards, and an equivalent level of protection can be found; or on the basis of a derogation.

As the article 45 of the GDPR establishes, transfers of personal data to a third country may take place where the Commission has decided that the third country, a territory, or one or more specified sectors within that third country ensure an adequate level of protection. An adequacy decision should be based on clear and objective criteria and, in particular, on the elements of the article 45 (2) of the GDPR. When assessing whether a third country '*offer*[s]

138 *See* Edgar, Laura, (2018), supra note 97, pp. 48-49.

guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union', the Commission should evaluate if that third country embeds the core principles of the GDPR and operates in the same spirt as the Charter of Fundamental Rights and other relevant international instruments.[139] Where an adequacy decision as been made by the Commission following the requirements of the article 45 of the GDPR, transfers of personal data do not require any specific authorization.[140]

In the absence of an adequacy decision, transfers of personal data to a third country are still possible in case the controller or processor has provided appropriate safeguards and, on the condition, that enforceable data subjects' rights and effective legal remedies for data subjects are available.[141] Such safeguards include legally binding and enforceable instruments between public authorities or bodies; binding corporate rules; standard data protection clauses, adopted by a supervisory authority and approved by the Commission; binding code of conduct together with enforceable commitments of the third country's controller or processor to apply these safeguards; and approved certification mechanisms together with enforceable commitments of the third country's controller or processor to apply these safeguards.[142] Where any appropriate safeguards are provided, and in case the requirements set under the article 46 of the GDPR are met, the controller or processor can transfer personal data to a third country, regardless of whether that transfer relies on the usage of blockchain-based applications or any other type of technology.[143]

As the article 49 of the GDPR implicitly acknowledges, there is a hierarchy between the legal grounds that allow the transfer of personal data to third countries. In this context, the abovementioned article only allows personal data to be transferred to a third country in case of the absence of an adequacy decision or of appropriate safeguards, on the basis of one of the conditions established under the article 49 (1) lit. (a) to (g) of the GDPR. Those conditions allow personal data to be transferred to a third country if the data subject has provided explicit consent after becoming aware of the risks of the transfer; if the transfer is necessary for the performance of a contract concluded between the data subject and the controller, or if such

139 Recitals 104 and 105 of the GDPR.
140 At the time of this study, the European Commission has recognized Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework) as providing adequate protection. To consult an updated list of the Commission's adequacy decisions: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, [accessed on the 24th of August of 2019].
141 Article 46 (1) of the GDPR.
142 Article 46 (2) of the GDPR.
143 *See* Finck, Michèle (2019), supra note 19, p. 90.

contract has been concluded in the interest of the data subject; if reasons of public interest justify the transfer; in case it is necessary to establish, exercise or defend legal claims; if the transfer is necessary to protect vital interests of the data subject; or, finally, if the transfer is made from a register which, according to Union or Member State law, is intended to provide information to the public and which is open to consultation. Although in most cases article 49 (1) of the GDPR provides compelling reasons for a transfer of personal data to a third country to be regarded as lawful, recitals 111 to 113 expressly recognize that those conditions only apply *'in residual cases where none of the other grounds for transfer are applicable*', considering that the transfers are occasional and, in most cases, necessary to achieve a legitimate purpose. In such cases and taking into consideration the other requirements of the article 49 of the GDPR, the controller or the processor may transfer personal data to a third country. However, considering the residual and occasional characteristics of those derogations, the article 49 of the GDPR does not provide an appropriate legal ground for all the cases dealing with considerable amounts of transfers of personal data to third countries.

Whereas blockchain-based applications rely on a wide P2P network, transfer of personal data to third countries or international organizations can generate legal tensions between blockchain and the GDPR, as the location of nodes cannot be controlled. On the contrary, blockchain-based applications that operate in a centralized manner can have a better control over the location of nodes and miners and decide to transfer or not personal data to a third country. Nevertheless, even on private and consortium blockchain-based platforms, nodes and miners can be located outside the European Union, as some types of platforms include the participation of subsidiaries or group companies. In such cases, a legal ground for such transfers still needs to be found and, as established under the article 13 (1) (f) of the GDPR, where personal data relating to a data subject are collected from her, the controller shall provide the data subject with information related to the intended transfer of personal data to a third country and the legal ground that lawfully allows such transfer.

5.BLOCKCHAIN: A TOOL TO ENHANCE COMPLIANCE WITH GDPR

As we have demonstrated previously, blockchain-based applications stand in tension with some provisions of the GDPR. Among others, these tensions are related to the identification of the data controllers and processors, the data subjects' rights and freedoms (namely the right of access, the right to rectification and the right to erasure), and the transfers of personal data to a third country or to an international organization. In part, this is due to the implicit GDPR's presumption that a single actor or a specific group of actors can be perfectly identified in all cases and qualified as either data controller or processor. However, as we also observed, the technological innovation made possible by blockchain technology profoundly changed the dynamics of the personal data processing, as in many cases, especially on public blockchain-based applications, the data subjects are themselves involved with data processing by copying, changing, sharing, and moving their own data through a (sometimes) wide and open P2P network. In face of that, a common critique has emerged, stressing out that even before the GDPR has entered into force and application, it was already outdated in relation to the innovative technologies such as blockchain.[144]

Although we tend to agree with such criticism, since, in certain circumstances, the expected technological neutral characteristic of the GDPR is not fully adapted to the latest technological advances, it can be argued that blockchain technology can be used to achieve the GDPR's objectives.[145] In fact, one could argue that blockchain technology has emerged precisely to give individuals more control over their data.[146] In this sense, some authors have highlighted the fact that blockchain technology and the GDPR share common values and principles with one another, which makes it possible to bring technology and law together.[147]

In view of the legal tensions that we have identified above, there are some solutions the legal literature has been studying in order to surpass them and to improve the level of protection the GDPR concedes to data subjects. In this context, blockchain-based applications architecture shall incorporate the principles of data protection by design and by default set under the article

144 *See* Cate, Fred H.; Kuner, Christopher; Lynskey, Orla; Millard, Christopher; Ni Loideain, Nora; and Svantesson, Dan Jerker B., (2018), supra note 18, p. 103. *See also* Finck, Michèle (2017), supra note 136, p. 34.
145 As per the Article 1 of the GDPR, the protection of natural persons with regard to the processing of personal data and the free movement of personal data are the two main objectives of the GDPR.
146 *See* Nakamoto, Satoshi, (2008), supra note 3, p. 1.
147 *See* Wirth, C. and Kolain, M. (2018), "*Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data*", Wolfgang Prinz and Peter Hoschka (eds) Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies Privacy by BlockChain Design, ISSN 2510-259, p. 1.

25 of the GDPR, in order to allow natural and legal persons to take the fully advantages of blockchain technology, without undermining data protection rules and the rights and freedoms of the data subjects.[148] The legal literature has conceptualized a few solutions and strategies that could be adopted to achieve the GDPR's objectives and, more generally, to ensure compliance with the regulation. Without prejudice to other solutions, we will now provide a brief overview of the two main solutions we believe to be more feasible to be used on blockchain-based applications to achieve and comply with the GDPR's objectives.

5.1 Using blockchain technology to improve data subjects' control over personal data

By laying down rules relating to the protection of natural persons with regard to the processing of their personal data, the GDPR recognizes that control over personal data is a crucial element of data protection.[149] As examined above, the accuracy principle and the data subjects' right of access, as well as the right to rectification and erasure, provide data subjects with different means to exercise control over their personal data. Recital 7 of the GDPR expressly foresees that '*natural persons should have control of their own personal data'*. The control over personal data implies that, at least, two main elements can be observed: first, data subjects shall have the possibility to monitor how their personal data is processed; and second, data subjects should have the opportunity to decide who should have access to their personal data.[150] However, it could be difficult to ensure the data subject has such control over her data, as in most cases, the data subject simply relies on the data controller or processor to process personal data in a lawful manner.[151]

In this context, blockchain technology, if properly designed to such ends, could be used to enable data subjects to exercise such control over their data. Indeed, there are a few use-cases that provide us with an idea on how blockchain-based applications can be used in this regard. Besides the Estonian experience on the health field, in which the patients can manage the access authorizations to their health data through a blockchain-based application,[152] there

148 *See* Lyons, T., Courcelas, L., and Timsit, K. (2018), supra note 51, p. 29. *See* also Hildebrandt, M. and Tielemans, L. (2013) "*Data Protection by Design and Technology Neutral Law*" Computer Law & Security Review 19, p. 516.
149 Article 1 (1) of the GDPR.
150 *See* Finck, Michèle (2019), supra note 19, p. 92.
151 *Ibid*.
152 *See* Priisalu, J. and Ottis, R. (2017) "*Personal control of privacy and data: Estonian experience*", 4 Health and Technology 441, *apud* Finck, Michèle (2019), supra note 136, p. 92.

are other blockchain-based applications such as Patientory and MedRec that give data subjects considerable control over their personal data.[153-154] In this regard, Faber *et al*. have conceived and proposed an interesting solution that, once incorporated on blockchain-based applications' design, would allow data subjects to better control access to their personal data.[155] The idea of a Blockchain-based Personal Data and Identity Management System (hereafter, BPDIMS) is to '*provide a holistic, personal data management tool to the user, meaning that the user of the system can expect full transparency and control over his personal data*'.[156] For such purpose, the BPDIMS's design contain three blockchain layers: a smart contract layer, an access layer, and a hash storage layer. The smart contract layer is used to store conditions for data exchanges between user and service providers or purchasers.[157] The access layer contains a '*a tool to ensure privacy*', through which it connects an offline storage with the blockchain, allowing the data subjects ' *to control and own their personal data, while service providers are guests with delegated permissions*".[158] Finally, the hash storage layer, which is used to store hashes of data that are created when *'personal data of the user is verified by certain trusted authorities like government organisations who could verify the user's personal details*'.[159]

Although the solution conceived by Faber *et al*. is not universal and it could not be used in all personal data processing cases, more importantly, it shows that it is possible to design blockchain-based applications in a manner that is compatible the GDPR, considering that the proposed BPDIMS also relies on the solution we present next.

5.2 The off-chain repository solution

Storing personal data into the blockchain arises numerous tensions with the GDPR. Even in cases where encryption techniques and hash functions are used to store personal data into

153 *See* https://patientory.com/technology/, [accessed on the 29th of August of 2019].
154 MedRec can be described as a *"combination of a social need with a technological enabler: a system that prioritizes patient agency, giving a transparent and accessible view of medical history*". As it explained on MedRec's website, "*Smart contracts act as an intelligent representation that links patients and providers to the addresses of existing medical records. Medrec does not 'store' the record directly; rather encodes metadata that allows records to be accessed securely by patients, unifying access to data across disparate providers. The metadata contains information about ownership, permission and the integrity of the data being requested*". *See* https://medrec.media.mit.edu/ [accessed on the 29th of August of 2019].
155 *See* Faber, B., Michelet, G., Weidmann, N., Mukkamala, R. R., and Vatrapu, R. (2019), "BPDIMS: A Blockchain-based Personal Data and Identity Management System", *in* Proceedings of the 52nd Hawaii International Conference on System Sciences, pp. 6859-6860.
156 *Ibid*.
157 *Ibid*.
158 *Ibid*.
159 *Ibid*.

the chain, these methods only pseudonymize personal data, which triggers the GDPR's applicability. In this context, it seems that blockchain technology and the GDPR stand in conflict with one another. The apparent antagonistic relationship between blockchain technology and the GDPR has been highlighted numerous times,[160] although further studies and experimentation indicate this technology may be suitable to achieve some of the GDPR's objectives and, when properly designed, it can comply with the data protection requirements.[161]

In this regard, the use of an off-chain repository provides us with a feasible solution that allows blockchain-based applications to operate in line with the GDPR's requirements. This approach suggests that personal data should be stored in an off-chain repository, while blockchain-based applications only store hashed links to the data residing on the off-chain repository (hashed data pointers). Such approach guarantees simultaneously that fragmented data becomes less attractive for hacking, while accessibility to the data in the database is not compromised.[162] Moreover, security measures can be adopted as the data subject's personal data could be stored in the off-chain repository in an '*encrypted form using symmetric encryption keys that are owned by the respective user who owns the data'*.[163]

The main advantages of such architecture are that, by storing hashed data pointers to data stored on the off-chain repository, data breaches can be detected more easily as any alteration made to the data stored on the off-chain repository can be spotted and, more importantly, since personal data is kept off the blockchain database, it allows data subjects to exercise their rights, namely, the right of access, the right to rectification, and the right to erasure.[164]

Many other solutions and technical approaches have been proposed as both areas of our study, blockchain technology and data protection, are being subject to further examination through interdisciplinary research.[165] Nevertheless, the solutions provided above show that

---

160 Jan Philip Albrecht, a member of the European Parliament, has reportedly stated that "*Certain technologies will not be compatible with the GDPR if they don't provide for [the exercising of data subjects' rights] based on their architectural design. This does not mean that blockchain technology, in general, has to adapt to the GDPR, it just means that it probably can't be used for the processing of personal data*". *See* Cate, Fred H.; Kuner, Christopher; Lynskey, Orla; Millard, Christopher; Ni Loideain, Nora; and Svantesson, Dan Jerker B., (2018), supra note 18, p. 103.

161 *See* Finck, Michèle (2019), supra note 19, p. 91.

162 *See* Faber, B., Michelet, G., Weidmann, N., Mukkamala, R. R., and Vatrapu, R. (2019), supra note 155, p. 6860.

163 *Ibid*.

164 Although hashed data pointers may persist on the blockchain database, this approach guarantees that personal data (including all instances of a private key for the encrypted data) can be deleted. *See* Bacon, J.; Michels, J.; Millard, C.; Singh, J. (2017), supra note 21, p. 48.

165 For instance, Accenture has recently registered a patent for an editable blockchain, in which blocks of data can be edited, rewritten or removed without break the chain. For more details, *see* Edgar, Laura, (2018), supra note 97, pp. 49-52.

blockchain-based applications can be designed to provide data subjects with more control over their data, by creating new forms of data management and sharing. The solutions exemplified above also prove that it is possible to use blockchain-based applications to achieve the GDPR's objectives.

6.CONCLUSION

This study has examined the application of the General Data Protection Regulation to blockchain-based applications. As observed, a universal definition of blockchain technology is hard to achieve, since different blockchain-based applications can present different structures and operate in different environments. Nonetheless, in order to create an immutable, tamper-evident record of transactions (or any other dataset) between parties, blockchain technology relies on two main components: hash functions and a public key infrastructure. While the former is used to guarantee data integrity by creating an immutable and tamper-evident record of transactions or any other dataset, the latter is used for identity authentication's purposes, with private keys being used to encrypt data and create digital signatures.

Blockchain-based applications can use this technology to create platforms with different features. In this study, we observed that blockchain-based applications can be qualified as public, private or consortium blockchains, depending on the roles of the users, nodes and miners; on permissions regarding the ledger of transactions' visibility and accessibility; and on the control over the blockchain-based application's underlying software.

Public blockchain-based applications are designed as open and permissionless platforms, where anybody can participate, either as a user, a node or a miner. Since these types of platforms are meant to operate in trustless environments, they rely on resource-intensive consensus protocols, such as the *Proof-of-Work*. Public blockchain-based applications tend to offer high transparency, strong data integrity, and high resilience. As observed, the users of this type of applications are identified by their public key or by their address, which makes it difficult to identify the user's real-world identity. However, in case users obtain their private and public key pair in an online wallet service, their real-world identity can be found easily, since many of these services can request a proof of the identity of their clients to comply with Know Your Client and Anti-Money Laundering laws.

On the contrary, private and consortium blockchain-based applications operate in a more centralized manner, where only a trusted third party or a few selected groups of participants can join the network and act as a user, a node or a miner. Because a certain level of trust can be found among the network in which these applications operate, private and consortium blockchains are designed as closed and permissioned platforms. Considering that only a few selected groups of participants can join these platforms, there is no need to implement a

resource-intensive consensus protocol, which enables these types of platforms to process a large number of transactions in an efficient way. Nevertheless, when compared with public blockchain-based applications, the users of private and consortium blockchain-based applications are easily identified since the participants of such platforms are selected and not everyone can join the network.

In regards to data protection, it was observed that there are numerous legal tensions between blockchain-based applications and the GDPR. At first sight, it appears that this is an antagonistic relationship, since the GDPR relies on the implicit assumption that data is controlled or processed by identifiable actors (data controllers or processors), in a centralized manner, while blockchain-based applications operate in a decentralized manner, with multiple actors and participants within a distributed network. Consequently, this study identifies and examines the three main categories of legal tensions that may occur, which relates to the determination of data controllers and processors; the exercise of the rights and freedoms of data subjects; and the transfers of personal to a third country or to an international organization.

This study has shown that the qualification of users, nodes and miners as (joint) controllers or processors has not reached a consensus within the legal literature. Although a case-by-case analysis is needed, taking into consideration the Article 29 Working Party criterion of the '*factual influence*' over the purposes and means of personal data processing, our study examined each blockchain-based applications type's participants, in order to qualify them into the categories established under the GDPR. Our findings suggest that users should be regarded as data controllers in a general manner, while nodes and miners tend to be qualified as data processors.

In relation to the data subjects' rights and freedoms set under the GDPR, it has been shown that, on the public blockchain-based applications, data subjects are enable to exercise their rights, namely the right of access (article 15), the right to rectification (article 16), and the right to erasure (article 17). On the contrary, on private and consortium blockchain-based applications it is easier for data subjects to exercise their rights, although the immutable feature of blockchain-based applications could pose serious challenges for data controllers to comply with such requests.

Finally, this study observed that, on public blockchain-based applications, personal data could be transferred to a third country or an international organization without relying on any legal basis the GDPR provides. By contrast, the operators and participants of private and consortium blockchain-based applications are in a better position to control the location of

nodes and miners and, for such reason, these types of applications can comply with the transfer rules set under the articles 44 to 49 of the GDPR.

The study has also highlighted possible solutions for blockchain-based applications to comply with GDPR's requirements and to help achieve its objectives. If properly designed, blockchain-based application could be used to improve data subjects' control over their personal data, an objective that GDPR clearly establishes under its recital 7. The off-chain repository solution also shows that it is possible to take full advantage of blockchain technology without jeopardizing the data subjects' rights and freedoms.

Although this study's findings allow a first approach to these matters to be taken by legal professionals, researchers and students, further interdisciplinary research on the blockchain-based applications' technical structure, design and governance is still needed in order to achieve compliance with GDPR's requirements. On the other hand, an interdisciplinary approach is also needed at the policy-making's level. Legislators and regulators should find new ways to cooperate with tech developers and entrepreneurs in order to effectively regulate the personal data processing within blockchain-based applications, mitigating the legal uncertainties related to their use and allowing the development of the European technological market, while protecting the rights and freedoms of data subjects.

7.BIBLIOGRAPHY

Books

Bashir, I., (2017), "Mastering blockchain", Packt Publishing Ltd

Nian, L., Chuen, D. (2015), "Introduction to Bitcoin", Handbook of Digital Currency, Chapter 1.

Reid, F. and Harrigan, M., (2013), "An analysis of anonymity in the bitcoin system", Security and privacy in social networks, Springer, New York

Case Law

ECJ Cases C-293/12 and C-594/12, Digital Rights Ireland, EU:C:2014:238, 8 April 2014

ECJ C-101/01, Bodil Lindqvist, EU:C:2003:596, 6 November 2003

ECJ Case C-131/12, Google Spain, ECLI:EU:C:2014:317, 13 May 2014

ECJ Case C-230/14, Weltimmo, EU:C:2015:639, 1 October 2015

Guidelines

Article 29 Working Party, Opinion 04/2007 on the concept of personal data (WP 136) 01248/07/EN

Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169) 00264/10/EN

Article 29 Working Party, Opinion 03/2013 on purpose limitation (WP 203) 00569/13/EN

Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (WP 216) 0829/14/EN

Commission Nationale Informatique et Libertés, 'Premiers Éléments d'analyse de la CNIL: Blockchain' (September 2018)

Journals

Bacon, Jean and Michels, Johan David and Millard, Christopher and Singh, Jatinder, (2017) “Blockchain Demystified”, Queen Mary School of Law Legal Studies Research Paper No. 268/2017

Berberich, Matthias and Steiner, Malgorzata (2016), “Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers”, 2 Eur. Data Prot. L. Rev

Biryukov, A., Khovratovich, D. and Pustogarov, I., (2014),” Deanonymization of clients in Bitcoin P2P network” in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security

Bonneau, J., Miller, A., Clark, J., Narayanan, A., A. Kroll, J., and Felten, E., (2015) “SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies”, IEEE Symposium on Security and Privacy

C., Henry, (2017) “Blockchain: Disrupting Data Protection?”, Privacy Law and Business International Report, November 2017; University of Hong Kong Faculty of Law Research Paper No. 2017/041

Cate, Fred H.; Kuner, Christopher; Lynskey, Orla; Millard, Christopher; Ni Loideain, Nora; and Svantesson, Dan Jerker B., (2018), "Blockchain versus Data Protection", International Data Privacy Law, Volume 8, Issue 2

Crosby, M., Nachiappan, Pattanayak, P., Verma, S., and Kalyanaraman, V., (2016), “Blockchain Technology: Beyond Bitcoin”, Applied Innovation Review, Issue No 2

D. Chaum (1983) “Blind Signatures for Untraceable Payments, Advances in Cryptology”, Proceedings of the Springer-Verlag Crypto'82, Vol. 3

Faber, B., Michelet, G., Weidmann, N., Mukkamala, R. R., and Vatrapu, R. (2019), “BPDIMS: A Blockchain-based Personal Data and Identity Management System”, in Proceedings of the 52nd Hawaii International Conference on System Sciences

Fabiano, N. (2018), “Blockchain and Data Protection: The Value of Personal Data”, J. Systemics, Cybernetics & Informatics

Finck, Michèle (2019), “Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?”, Panel for the Future of Science and Technology, European Parliamentary Research Service, Scientific Foresight Unit

Finck, Michèle, (2017), “Blockchains and Data Protection in the European Union”, Max Planck Institute for Innovation & Competition Research Paper No. 18-01.

Giannopoulou, Alexandra and Ferrari, Valeria, (2016), “Distributed Data Protection and Liability on Blockchains”, in Internet Science: 5th International Conference proceedings, Vol. 2. Workshops; Amsterdam Law School Research Paper No. 2019-06; Institute for Information Law Research Paper No. 2019-03.

Hildebrandt, M. and Tielemans, L. (2013) "Data Protection by Design and Technology Neutral Law" Computer Law & Security Review 19

Ibáñez, Luis-Daniel, O'Hara, Kieron and Simperl, Elena (2018), “On Blockchains and the General Data Protection Regulation”, EU Blockchain Forum and Observatory

Lyons, T., Courcelas, L., and Timsit, K. (2018), “Blockchain and the GDPR”, European Union Blockchain Observatory and Forum

Maurer, B., Nelms, T. C., & Swartz, L. (2013), “When perhaps the real problem is money itself! the practical materiality of Bitcoin”, Social Semiotics, 23(2)

Priisalu, J. and Ottis, R. (2017) “Personal control of privacy and data: Estonian experience”, 4 Health and Technology 441

Sater, Stan (2017), “Blockchain and the European Union's General Data Protection Regulation: A Chance to Harmonize International Data Flows”, Social Science Research Network

Schwerin, Simon (2018) “Blockchain and Privacy Protection in the Case of the European General Data Protection Regulation (GDPR): A Delphi Study”, The Journal of The British Blockchain Association, Vol. 1, Issue 1

Truong, N., Sun, K., Lee, G., Guo, Y. (2019) “GDPR-Compliant Personal Data Management: A Blockchain-based Solution”, IEEE transaction on information forensics and security

Vetter, Greg R., (2004) "'Infectious' Open Source Software: Spreading Incentives or Promoting Resistance?", Rutgers Law Journal, University of Houston Law Center, No. 2004-A-11

Wirth, C. and Kolain, M. (2018), "Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data", Wolfgang Prinz and Peter Hoschka (eds) Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies Privacy by BlockChain Design

Wright, Aaron and De Filippi, Primavera, (2015) "Decentralized Blockchain Technology and the Rise of Lex Cryptographia", Social Science Research Network

Zheng, Z., Xie, S., Dai, H.N., Chen, X. and Wang, H., (2017), "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends". In 2017 IEEE International Congress on Big Data

Legislation

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

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

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)

Thesis

Edgar, Laura, (2018), "*Blockchain and data protection: evaluating the legal compatibility of blockchain technology with the general data protection regulation*", Queen Mary University of London, Centre of Commercial Law Studies

Websites

Khatri, Yogita, (December 28, 2018) "Electrum Wallet Attack May Have Stolen As Much as 245 Bitcoin" in https://www.coindesk.com/electrum-wallet-attack-may-have-stolen-as-much-as-245-bitcoin

Whitepapers

Nakamoto, Satoshi, (2008) "*Bitcoin: A Peer-to-Peer Electronic Cash System*", www.bitcoin.org

CYBERLAW

by CIJIC

OPINIÃO

A GESTÃO DOCUMENTAL COMO A ALAVANCA À CONFORMIDADE DO REGULAMENTO GERAL DE PROTECÇÃO DE DADOS (RGPD)

SOFIA PINA [1]

1 Arquivista. Contactos:. sofia.opina@gmail.com

O RGPD e a gestão documental são alavancas mútuas porque "arquivar, preservar e controlar dados pessoais" é o mesmo processo que "arquivar, reter e controlar documentos relevantes": precisamos de conhecer a vida útil da informação e justificar a sua duração, caso contrário, vamos eliminá-los indiscriminadamente. Irrecuperavelmente.

De um lado apresenta-se-nos o RGPD, como baluarte da Protecção de dados de carácter pessoal dos cidadãos do espaço europeu; do outro lado, a gestão documental e a abordagem empresarial para o controlo da informação ao longo do tempo. Entre ambos existe a ténue linha da recuperação de informação.

Foquemo-nos **nos prazos de conservação**.

Tudo começa na recolha.

O RGPD contém disposições específicas sobre a documentação das atividades em processamento. Os dados pessoais incluem dados recolhidos diretamente através de formulários, bem como todos aqueles que cedemos. Mesmo que de forma involuntária. O RGPD requer uma recolha de dados pessoais "lícita e legal". A recolha "lícita" é baseada no consentimento prévio e na explicação da legitimidade dessa mesma recolha (prospeção comercial, marketing, estudo, estatística, etc. ...). A documentação RGPD deve registar o consentimento, como garantia de rastreabilidade ao longo do tempo, e o princípio da proporcionalidade de recolha apresentado é o de manter a necessidade estrita. Os registos das atividades devem manter-se como fins do processamento, de partilha de dados e de retenção, uma vez que a entidade reguladora, se assim o entender, poderá requerer a sua disponibilização.

A gestão documental é, aqui, precursora na definição dos prazos de conservação ao considerar os dados a partir do seu momento de produção e não de registo. O RGPD enuncia

períodos de retenção de dados, mas não refere que estes mesmos prazos estejam associados aos processos de negócio.

Se nos focarmos apenas na duração da utilização operacional, corremos o risco de nos esquecermos da salvaguarda dos requisitos de evidências! O mesmo é dizer que os dados individuais também pertencem a bases de dados com valor de evidência de longo prazo.

Com a promulgação da Lei n.º 58/2019 de 8 de Agosto, que assegura a execução na ordem jurídica nacional do Regulamento 2016/679 do Parlamento e do Conselho Europeus, o prazo de conservação de dados pessoais é fixado no artigo 21.º. Tal como a gestão documental já o executava, o prazo de conservação de dados pessoais é fixado por norma legal ou regulamentar, e na sua falta, a finalidade será justificada pela necessidade.

Desde que as organizações adoptem medidas técnicas e organizativas adequadas às garantias dos titulares dos dados, o fim justificará a conservação permanente ou num espaço de tempo mais dilatado, desde que o arquivo seja de interesse público, para investigação científica, histórica ou estatística[1].

O artigo 26.º da Lei n.º 58/2019, *glosou* a redação da *L.A.D.A. – Lei de Acesso aos Documentos Administrativos* – Lei n.26/2016 de 22 de Agosto, no que concerne aos documentos administrativos com dados pessoais.

O artigo 31.º da Lei n.º 58/2019 garante ao arquivo de interesse público para os fins de investigação identificados, a conservação de dados, salvaguardando os interesses dos titulares, através de técnicas de minimização, de anonimização ou ainda de pseudonimização. Ou seja, *mantem-se em vigor* a redação atual do Decreto-Lei 16/93 de 23 de Janeiro, no que se refere ao tratamento de dados pessoais para fins de arquivo de interesse público.

Os processos de documentação permitem cumprir vários requisitos do RGPD, além de melhorar a gestão de dados, já que são essas as obrigações do responsável pelo tratamento de dados (*Data Controller)* e do processador *(Data Processor*).

1 Ver *Orientações sobre Protecção de Dados nos Arquivos - Orientações do GEA sobre a implementação do Regulamento Geral de Proteção de Dados no setor dos arquivos, Título original: Guidance on data protection for archive services. EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector, Autor*: © European Archives Group, Tradução da autora.

Continuando no artigo 21º, sempre que houver a necessidade de comprovar a obrigação contratual, a conservação num prazo dilatado é permitida, desde que fundamentada, salvaguardando os direitos correspetivos.

A minimização e /ou a anonimização dos dados no momento da recolha é apenas um dos aspetos. Se considerarmos um serviço como a parte exposta de um conjunto de realizações de trabalho (definição de arquitetura empresarial), o exercício não se limita à catalogação dos serviços, mas à caracterização dos processos que os realizam. Por exemplo, a finalidade dos tratamentos é mais adequada se representada pelos processos (ou seja, as realizações de trabalho) do que se pelos serviços (a parte exposta). O documento faz parte de um processo e é segundo a MEF/LC *(Macroestrutura funcional / Lista Consolidada*), que os prazos e destinos da informação são definidos por processo, ou seja, é o contexto de negócio que determina as regras para gerir as peças de informação (o *documento).*

Em termos de ferramentas tecnológicas, a proteção de dados por *design* deverá fazer parte da transformação digital de uma empresa, além de permitir funcionar como garante, a quem gere as aplicações, que está a gerir dados recolhidos desde o início da sua produção.

A boa gestão da informação exige uma clara definição de perfis bem como a correta segmentação de processos de negócio, evitando o uso de dados recolhidos a um cliente num outro contexto, uma vez que a avaliação, e a posterior classificação de dados, só será válida caso os dados sejam recolhidos de forma lícita, nos termos do RGPD.

As auditorias e os exercícios de mapeamento de dados, suportam-se no processamento da documentação das atividades, e todos esses registos devem ser mantidos por escrito (ainda que em suporte digital), e atualizados de forma a refletirem sempre o processamento das atividades atuais. E em conformidade com a lei.

É importante que o sistema informático de gestão de dados pessoais se baseie em regras de arquivo (*a gestão documental*), de preferência actuais, cumprindo as leis em vigor e conhecidas pelos vários atores da empresa.

Os arquivistas / gestores documentais, por tudo isto, apresentam-se assim como os mais avalizados, se não os únicos, para fazer cumprir corretamente a legislação no tocante aos prazos de conservação dos dados pessoais.