RANSOMWARE

Claudio Maia de Barros Eduardo Nepomuceno de Sousa Eduardo Fantinati Menezes Juliana Gomes dos Santos

Abstract: This article aims to explain how the technological evolution used for illicit purposes, specifically Ransomware, can bring serious financial and social losses, as well as the importance of the Prosecution's performance in this new form of criminal activity.

Keywords: Ransomware; Bitcoin; Cases; General Law of Data Protection (Lei Geral de Proteção de Dados).

INTRODUCTION

The Public Prosecution Office has assignments established on the Federal Constitution and the infraconstitutional legislation to defend the legal order, democratic regime, and social and individual rights.

The institutional acting is often marked by transdisciplinarity, given the entanglement of themes and subjects of the activities, when in concrete exercise.

As the holder of the criminal prosecution, the Public Prosecution Office is responsible for promoting all the necessary acts to fulfil its duties, especially those related to the investigation phase.

While on the more committed crimes, there is evident police (local and federal) expertise for the elucidation, the reality is different when the conduct involves peculiar aspects, like the one that offends the environment, elderly, women, children and teenagers, cultural and public property, among other diffuse interests.

In this specific scenario, the Public Prosecution Office becomes a protagonist due to, mainly, the model adopted, *interna corporis*, for the distribution of its assignments, so that the defense of diffuse rights, in a specialized and systematized way, is still innovated in some organs and institutions, is promoted by the Parquet since the Constitution of 1988 and even before that, considering the validity of the Public Civil Action Law (Lei de Ação Civil Pública - 7.347/85)

A good example of the specialized acting with transdisciplinarity elements is in the Corporate Law Courts, where, at first or in most cases, the activity is related to the follow-up of bankruptcy and judicial reorganization proceedings.

The bankruptcy and judicial reorganization proceedings involve, however, discussions not only from Corporate Law but also, in the majority of cases, it's criminal and civil repercussions, given the possibility of previous illegal activities, such as unfair competition, money laundering, consumer injury, fraud on creditors, and others.

In this bias, the Public Prosecution Office's attention is not focused on merely formal aspects, demanding a comprehensive investigation of the factual and legal panorama that preceded the bankruptcy and judicial reorganization proceedings to prevent the improper use of these legal institutes.

The recent "Car Wash" ("Lava Jato") operation, for example, fomented many proceedings of that nature in a way to shuffle criminal, corporate and political discussions and impose a cautious look from the one that, at first, would be a mere fiscal of the legal order.

Thus, Prosecutors must know not only the technical concepts of Corporate Law but also each company's operation model and accounting and commercial reality so that they can exercise their assignments with safety to notice management distortions and possible illegalities committed by associates, managers and others.

RANSOMWARE AND BITCOINS

A practice that has been creating undeniable discomfort is Ransomware, popularly known as the data hijack or digital hijack.

In fact, it is malware (malicious software) that encrypts files and documents, local and online, to hinder access to obtain an illegal advantage.

In a historical panorama of the theme, it is essential to point out that the Internet emerged in the United States of America in 1969. Still, until then, it was directed exclusively to North American defense in the Cold War to ensure the communication between the scientists and military during the bombings.

In the USA, the commercial use of the Internet was authorized in 1987, and in 1989, the first documented Ransomware attack happened.

This first attack was fulfilled via floppy disks distributed by "Joseph Popp, PhD, AIDS researcher, claiming that the disks contained a program that analyzed individuals' risk of contracting AIDS. However, the disks also contained a malware

program that initially stayed inactive in the computers, only activating after the computer was booted up 90 times. Once the limit of 90 boots was reached, the malware showed a message demanding the payment of $189 and $378 as a software lease. This Ransomware attack was known as AIDS Trojan or PC Cyborg."

The primary Ransomware attacks were: WannaCry, 2017; BadRabbit; Cerber; Darkside; Crysis; Locky; Jigsaw; Petya; GoldenEye; Reveton; Maze ransomware.

This type of data hijack can have as a victim a person, a company or even a governmental institution; Brazil is on the list of the ten countries with more Ransomware victims, and the leading cases were: JBS (food company), Renner, Superior Court of Justice, Department of Health and Department of the Treasury.

The perpetrators of this crime can have various purposes. For example, in 2020, the Superior Court of Justice[1] case caused the suspension of deadlines and internal activities given its magnitude because all the databases and backups were encrypted, making the system unavailable to the internal and external public[2].

Private companies, in the majority of cases, are the favorite targets due to the facility of getting payment for the rescue or due to illicit competitive practices.

In another emblematic case that took place in May of 2021, Colonial Pipeline, an American pipeline company hosted in Houston, Texas, suffered a cyberattack that impacted all of its computer networks, and it was considered the most significant attack that occurred in that country, forcing the company to pay for the rescue in cryptocurrency *(bitcoin)*[3].

The Public Prosecution Office's intervention in combatting and preventing the illicit imposes even more knowledge about the cryptocurrency market, especially bitcoin, as it is the type of rescue usually required.

Illicit cryptocurrency negotiations, especially bitcoin, happen in the so-called "deep web" or "dark web", a term created by Mike Bergman in 2000[4], given the fragility of the control mechanisms and tracking difficulty.
Vanson Bourne[5] has already researched the progressive increase of cases, which only confirms how current the theme is.

In Brazilian Law, the practice is typified in articles 154-A, 154-B, 171, paragraphs 2º-A and 2º-B, and 266, of the Brazilian Penal Code (BPC)

---

[1] Disponível em https://g1.globo.com/politica/noticia/2020/11/04/stj-aciona-pf-para-apurar-possivelataque-de-hackers-ao-sistema-do-tribunal.ghtml (acesso em 18 de abril de 2022).
[2] Disponível em https://www.tecmundo.com.br/seguranca/206233-ataque-hacker-ter-atingido-stj-pfinvestiga.htm (acesso em 18 de abril de 2022).
[3] https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack (acesso em 18 de abril de 2022).
[4] Disponível em https://www.moneytimes.com.br/fabricio-alexandre-qual-e-a-relacao-entre-obitcoin-e-a-deep-web/ (acesso em 18 de abril de 2022).
[5] Disponível em https://assets.sophos.com/X24WTUEQ/at/hr6gj5b5v8btxpq68xqh34/sophos-itsecurity-team-2021-beyond.pdf (acesso em 18 de abril de 2022).

Besides that, it is cogitated about the viability of imputation of qualified theft (article 155, §4º-B BPC), extorsion (article 158 BPC) and unfair competition (article 195, XII, Law nº 9.279/1996).

As it is a crime without borders, the coping measures come from countries interested in combatting and preventing the illicit, such as the United States of America and the European Community.

In Europe, for example, NMR (No More Ransom) was created, a system that helps Ransomware victims recover access to their data without paying for the rescue[6].

In a meeting that took place on October 2021, convened by the White House[7], 31 countries, Brazil among them, committed to adopting measures to combat cybernetic attacks, including the adoption of measures against money laundering and in favor of collaboration for investigations. Furthermore, the Global Conference[8]against Ransomware established four goals: improve the detection of these cybernetic crimes, increase the resilience of networks and public and private companies to attacks, end the impunity that protects cryptocurrency, typically used in the payment for the rescue, and increase the international cooperation in the combat to cybercrime.

It is essential to mention that the Law Project nº 3.825/2019, which creates rules for the national market of cryptocurrency, has been discussed in the National Congress.

The Brazilian participation serves as encouragement so that the organs of control, combat and repression of the illicit, especially the Public Prosecution Office, can raise effective acting instruments, besides the larger facility to access international cooperation.

According to specialists, considering the individual acting, some measures to avoid the attacks or minimize the damages are doing backups, installing antivirus and preventing access to suspicious icons.

---

[6] Disponível em https://www.europol.europa.eu/operations-services-and-innovation/publicawareness-and-prevention-guides/no-more-ransom-do-you-need-help-unlocking-your-digital-life (acesso em 18 de abril de 2022).

[7] Disponível em https://www.convergenciadigital.com.br/Seguranca/Brasil-participa-de-conferenciaglobal-contra-ransomware-na-Casa-Branca-58431.html?UserActiveTemplate=mobile (acesso em 18 de abril de 2022).

[8] Id.

GENERAL LAW OF DATA PROTECTION (LEI GERAL DE PROTEÇÃO DE DADOS)

Under the legal aspect, in Brazil, ransomware attacks must be understood considering Law nº 13.709, from August 14 of 2018, more known as General Law of Data Protection (LGPD – Lei Geral de Proteção de Dados), that started to have validity only two years after it was published, at least the majority of the provisions.

LGPD regulates the treatment of personal data, especially in digital media, to protect fundamental rights, particularly the right to privacy.

This Law brings important conceptual provisions necessary to the comprehension of its prescriptions, defining, for example, that the "holder" is the person that has personal data as the object of treatment; the "controller" is the person responsible for the decisions regarding the treatment of personal data; "operator" is the person that does the treatment of personal data in the name of the controller; and "national authority" is the public administration organ responsible for looking after, implementing and supervising the enforcement of this Law all over the national territory (article 5º, V, VI, VII and XIX).

LGPD has some provisions that impose obligations to those responsible for dealing with personal data from their clients and others, establishing a strict civil and administrative responsibility regime as a consequence of not fulfilling those obligations.

In this regard, for example, there is a provision that imposes on the controller the duty of communicating to the national authority and the data holders, eventual security incidents - ransomware attacks, for example - that can lead to risks or relevant damages to them (article 48), a necessary action to alert the indirect victims of the risk they are exposed to, making it possible for them to adopt immediate measures to mitigate the risks of suffering material and immaterial damage.

Regardless of that, the law assigns, to the "controller" and to the "operator" the obligation of repairing the damages caused by the treatment of personal data in offense to the data protection legislation, with the possibility of reversal of the burden of proof in favor of the data holder if the allegation is likely to be accurate, if there is hypo sufficiency, or if the proof production by the holder is exceedingly onerous (article 42, caput and §2º).

On the other hand, LGPD withdraws the possibility of blaming the personal data treatment agents when they prove, alternatively: a) that they didn't participate in the personal data treatment; b) that there was no offense to the data protection legislation; or c) that the damage occurred due to sole fault from the data holders or others (article 43).

This last hypothesis has particular relevance in the debate about the ransomware attacks that are increasingly occurring to companies in the previous years because the existence of "sole fault" depends on the analysis of the measures adopted by the companies to protect the personal data under their responsibility, reducing the success chances of virtual crimes practiced by others, such as the ransomware attacks.

In this regard, article 44 of LGPD establishes that the personal data treatment will be irregular if it doesn't observe the legislation or if it doesn't provide the safety that the data holder might expect, considering the relevant circumstances, especially the way it is done, the results and the risks that are reasonably expected, and the personal data treatment techniques available by the time.

As one might see, the law uses many undetermined legal concepts to treat the responsibility regime, leaving a wide margin for the judges to decide with motivated discretion in concrete cases.

This discretion tends to be reduced by the implementation of minimum technical standards for the adoption of data security measures, an activity reserved for the federal organ created by LGPD itself, called Data Protection National Authority (Autoridade Nacional de Proteção de Dados – article 46, §1º c/c articles 55-A to 55-L). By the way, the national authority has been editing normative acts to regulate LGPD, an essential measure, so the application of the law respects legal security[9].

Concurrently to the obligation of repairing damages caused to their clients and others (civil responsibility), LGPD establishes a system of the administrative burden that reaches data treatment agents in case of offense to the provisions in this law.

The administrative sanctions that the national authority may apply, considering the established legal criteria and the hierarchically inferior to the law regulation to be edited, include a "warning", with the designation of a deadline to adopt corrective measures, OK up to 2% (two per cent) of the company revenue in the last year,

[9] Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes, acesso em 20/04/2022.

limited to R$50.000.000,00 (fifty million reais) for offense, prohibition to do activities related to data treatment, among others (article 52).

Although this law was necessary to establish the obligations of people (individuals and companies) that deal with personal data from their clients and others, as well as the consequences in case of not fulfilling those obligations, it is a fact that LGPD has been pointed as a factor of increment of ransomware attacks against companies.

Currently, criminals behind these attacks are not just encrypting the companies' files but also trying to extract the institution's data, threatening the managers to release the files' content in case the payment for the rescue isn't made[10].

CONCLUSION

The goal of the present article was to draw attention to the technological evolution and how criminal/illicit acting via the internet, especially regarding ransomware, can cause severe social and financial losses, as well as the importance of improvement and specialization in the rule of the Public Prosecution Office to accomplish its constitutional duty.

REFERENCES

BRASIL, Lei n 13.709, de 14 de agosto de 2018.
Disponível em https://valor.globo.com/legislacao/noticia/2021/10/04/ransomware-ealgpd.ghtml, Felipe Palhares, acesso em 20/04/2022;
https://www.gov.br/anpd/ptbr/documentos-e-publicacoes, acesso em 20/04/2022;
https://g1.globo.com/politica/noticia/2020/11/04/stj-aciona-pf-para-apurar-possivelataque-dehackers-ao-sistema-do-tribunal.ghtml (acesso em 18 de abril de 2022); https://www.tecmundo.com.br/seguranca/206233-ataque-hacker-ter-atingido-stjpfinvestiga.htm (acesso em 18 de abril de 2022);
https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack (acesso em 18 de abril de
2022); https://assets.sophos.com/X24WTUEQ/at/hr6gj5b5v8btxpq68xqh34/sophos-itsecurityteam-2021-beyond.pdf (acesso em 18 de abril de 2022);
https://www.moneytimes.com.br/fabricio-alexandre-qual-e-a-relacao-entre-o-bitcoin-e-a-deepweb/ (acesso em 18 de abril de 2022);

[10] Disponível em: https://valor.globo.com/legislacao/noticia/2021/10/04/ransomware-e-algpd.ghtml, acesso em 20/04/2022.

https://www.europol.europa.eu/operations-servicesand-innovation/public-awarenessand-prevention-guides/no-more-ransom-do-you-need-helpunlocking-your-digital-life
(acesso em 18 de abril de 2022);
https://www.convergenciadigital.com.br/Seguranca/Brasil-participa-de-conferenciaglobalcontra-ransomware-na-Casa-Branca-58431.html?UserActiveTemplate=mobile
(acesso em 18
de abril de 2022); https://cointelegraph.com.br/news/chainalysis-only-1-of-1trilliontransacted-in-crypto-in-2019-was-illicit (acesso em 18 de abril de 2022) e www1.folha.uol.com.br (acesso em 19/04/2022).
LISKA, Allan; GALLO, Timothy. Ransomware (Defendendo-se da Extorsão Digital). 1ª ed. São
Paulo: Novatec Editora Ltda., 2017.

REFERÊNCIAS BIBLIOGRÁFICAS

AVERGUN, Jodil; **COHAN,** Douglas. *Explaining the Inexplicable: The Perks and the Perils of Proffer Sessions and Best Practises for Explaining it All to Your Client.* Disponível:https://www.cadwalader.com/uploads/books/0a31f986d2926e6929e74e27c97093a8.pdf. Acesso em: 31 de mar. de 2022.

BURNHAM, GOROKHOV. *Understanding Proffer in Federal and White Collar Criminal Cases: frequently asked questions*. Disponível em: <https://www.burnhamgorokhov.com/criminal-defenseresources/white-collar-crimes/understanding-proffers-in-federal-and-white-collar-criminal-cases/ > Acesso em : 05 de abr. de 2022.

GALLUZZO, Matthew J. *Federal Proffer Meetings and Agreements.* 03.03.2022. Disponível em:<https://www.gjllp.com/news/amp/federal-proffer-meetings-and-agreements/> Acesso em : 14 de abr. de 2022.

GORIN. Dmity. *Proffer Agreement in a Federal Criminal Case*. Disponível em <https://www.thefederalcriminalattorneys.com/proffer-agreement-in-a-federal-criminal-case/> Acesso em : 12 de abr. de 2022.

MARTIN, Ingrid. **DISTEFANO**, Michael. *A Survey of Federal Proffer Agreements: the shortcomings and pitfalls in the Government's Promised Protections*. The Champion.2020.Disponível em: http://www.toddweld.com/files/documents>. Acesso em 17.03.2022.

OBERHEIDEN P.C. Litigation, Defense, Trials & Compliance. *What is a Proffer Agreement.* 04 de abr. de 2022. Disponível em <https://federal-lawyer.com/what-is-a-proffer-agreement/> Acesso em: 10 de abr. de 2022.

USA.SECURITIES AND EXCHANGE COMISSION DIVISION OF ENFORCEMENT. *Enforcement Manual.* 28 de nov. de 2017. Disponível em : <https://www.sec.gov/divisions/enforce/enforcementmanual.pdf > Acesso em : 10.03.2022.

WORDPRESS.*Idiomation.*Disponível<https://idiomation.wordpress.com/2013/06/28/queen-for-a-day/> Acesso em : 15 de abr. de 2022.

UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT. *United States v. Lyle*, 919 F.3d 716, 732-35 (2d Cissr. 2019).Casetext. Disponível em: <http://casetext.com/case/united-states-vlyle> Acesso em: 16 de abr.de 2022.

UNITED STATES COURT OF APPEALS FOR THE THIRD CIRCUIT. *United States v. Merz*, 396 F. App'x 838 (3d Cir. 2010). Casetext. Disponível em: <http://casetext.com/case/us-v-merz> Acesso em: 17 de abr.de 2022.
UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT. *United States v. Mezzanatto*, 513 U.S. 196, 200-18 (1995). Casetext. Disponível em: <http://casetext.com/case/united-states-vmezzanato> Acesso em: 16 de abr. de 2022.
UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT. *United States v. Rosemond*, 841 F.3d 95, 107-10 (2d Cir. 2016). Casetext. Disponível em: <http://casetext.com/case/united-statesv-rosemond> Acesso em: 16 de abr. de 2022.
UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT. *U.S. v. Velez*, 354 F.3d 190 (2d Cir. 2004). Casetext. Disponível em: <http://casetext.com/case/us-v-velez> Acesso em: 17 de abr.de 2022.

INTRODUÇÃO

O Ministério Público possui atribuições previstas tanto na Constituição Federal quanto na legislação infraconstitucional para a defesa da ordem jurídica, regime democrático e direitos sociais e individuais indisponíveis.

A atuação institucional é marcada, não raras vezes, pela transdisciplinaridade, dado o entrelaçamento de temas e matérias quando do exercício, em concreto, das atividades.

Como titular da ação penal, compete ao Ministério Público a promoção de todos os atos necessários para o fiel cumprimento de seu *múnus*, destacadamente aqueles relacionados à fase de investigação.

Se, nos crimes mais comumente praticados, existe evidente *expertise* das polícias, civil e federal, para sua elucidação, a realidade se mostra distinta quando a conduta envolve aspectos peculiares, tais como aquela que ofende o meio ambiente, idoso, mulher, criança e adolescente, patrimônios público e cultural, consumidor, dentre outros interesses difusos.

Nesse cenário específico, o Ministério Público se torna protagonista em razão, sobretudo, do modelo adotado, *interna corporis*, para distribuição de suas atribuições, de modo que a defesa dos direitos difusos, de forma especializada e sistematizada, ainda inovada em determinados órgãos e instituições, é promovida pelo *Parquet* desde a promulgação da Constituição de 1988 e até antes disso, haja vista a vigência da Lei de Ação Civil Pública (7.347/85).

Um bom exemplo da atuação especializada com elementos da transdisciplinaridade está na atuação junto às Varas de Direito Empresarial onde, a princípio ou na maior parte das vezes, a atividade relaciona-se ao acompanhamento de processos falimentares e de recuperação judicial.

Os processos de falência e de recuperação judicial envolvem, todavia, discussões não só de Direito Empresarial, como também em grande parte, a sua repercussão criminal e cível, propriamente ditas, ante a possibilidade de práticas ilícitas anteriores, tais como concorrência desleal, lavagem de dinheiro, lesão a consumidores, fraude contra credores, dentre outras.

Nesse viés, a atenção do Ministério Público não se concentra em aspectos meramente formais, exigindo-se, ao contrário, ampla perquirição acerca do panorama fático-jurídico que antecedeu o processo de falência e recuperação judicial de forma a impedir o uso indevido de tais institutos jurídicos.

A recente operação "Lava Jato", à guisa de exemplo, fomentou diversos procedimentos de tal natureza, de modo a embaralhar discussões criminais, empresariais e políticas e a impor um olhar cauteloso daquele que, a princípio, seria mero fiscal da ordem jurídica.

Em tal quadro, denota-se que Promotores de Justiça devem conhecer não só os conceitos técnicos do Direito Empresarial, como, precipuamente, o próprio modelo de funcionamento de cada empresa, sua realidade comercial e contábil, para que possa exercer com segurança suas atribuições a fim de enxergar distorções de gestão e eventuais ilicitudes praticadas por sócios, gestores ou terceiros.

RANSOMWARE e BITCOINS

Uma prática que tem gerado inegável desconforto é o *Ransomware*, popularmente conhecido como sequestro de dados ou sequestro digital.

Em verdade, trata-se de um *malware* (software malicioso) que criptografa arquivos e documentos, locais e de rede, impedindo seu acesso com o objetivo de obtenção de vantagem ilícita.

Num panorama histórico sobre o tema é importante ressaltar que a Internet surgiu nos Estados Unidos da América em 1969, mas até então era voltada exclusivamente para a defesa norte americana na fase da Guerra Fria, pois visava garantir a comunicação entre os cientistas e militares durante bombardeios.

Nos EUA o uso comercial da Internet foi autorizado desde 1987 e em 1989 houve o primeiro ataque documentado de *Ransomware*.

Esse primeiro ataque foi realizado via disquetes distribuídos por "*Joseph Popp, PhD, um pesquisador da AIDS, alegando que os discos continham um*

programa que analisava o risco de um indivíduo de adquirir AIDS por meio de questionário. No entanto, o disco também continha um programa de malware que inicialmente permaneceu inativo nos computadores, ativando-se apenas depois que um computador foi ligado 90 vezes. Depois que o limite de 90 inicializações foi atingido, o malware exibiu uma mensagem exigindo um pagamento de $ 189 e outros $ 378 por um aluguel de software. Esse ataque de ransomware ficou conhecido como o ***Trojan*** *da* ***AIDS*** **,** *ou PC Cyborg*."

Os principais ataques de *Ransomware* foram: *WannaCry, em 2017; BadRabbit; Cerber; Darkside; Crysis; Locky; Jigsaw; Petya; GoldenEye; Reveton; Maze ransomware*.

Essa espécie de sequestro de dados pode ter como vítima pessoa física, jurídica e até instituições públicas, sendo que o Brasil está na lista dos dez países com maior número de vítimas do *Ransomware* e os principais casos foram: JBS empresa distribuidora de alimentos; Lojas Renner; Superior Tribunal de Justiça, Ministério da Saúde e o Tesouro Nacional.

Os praticantes de tal ilícito podem ter objetivos diversos. Em 2020, o caso do Superior Tribunal de Justiça[11] que gerou a suspensão de prazos e atividades internas dada a sua magnitude, posto ter sido criptografada toda a base de de dados, *backups*, tornando o sistema inacessível para o público interno e externo[12].

Empresas privadas, na maioria das vezes, tornam-se o alvo preferido, seja em razão da maior facilidade para pagamento dos resgates ou mesmo por práticas concorrenciais ilícitas.

Em outro caso emblemático, ocorrido em maio de 2021, a Colonial Pipeline, uma empresa americana atuante no ramo de oleodutos e situada em Houston, Texas, sofreu *cyberattack* que impactou toda sua rede de informática, o que foi considerado o maior ataque ocorrido naquele país, obrigando a empresa vítima efetuar pagamento do resgate em *criptomoeda (bitcoin)*[13].

A intervenção do Ministério Público no combate e prevenção ao ilícito impõe ainda o conhecimento acerca do mercado de *criptomoedas*, especialmente *bitcoin*, em razão de ser o tipo de resgate comumente exigido.

---

[11] Disponível em https://g1.globo.com/politica/noticia/2020/11/04/stj-aciona-pf-para-apurar-possivel-ataquede-hackers-ao-sistema-do-tribunal.ghtml (acesso em 18 de abril de 2022).

[12] Disponível em https://www.tecmundo.com.br/seguranca/206233-ataque-hacker-ter-atingido-stj-pfinvestiga.htm (acesso em 18 de abril de 2022).

[13] https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack (acesso em 18 de abril de 2022).

Negociações ilícitas de *criptomoedas*, em especial *bitcoins*, ocorrem na chama "deep web" ou "dark web", termo criado por Mike Bergman, em 2000[14], ante a fragilidade de mecanismos de controle e dificuldade de rastreamento.

O aumento progressivo de casos já foi objeto de pesquisa, realizada pela Vanson Bourne[15], o que somente confirma a atualidade do tema.

No direito brasileiro a prática encontra previsão típica nos artigos 154-A, 154-B, 171, parágrafos 2º e 2º e 266, do Código Penal Brasileiro.

Cogita-se, ainda, acerca da viabilidade de imputação de furto qualificado (art. 155, § 4º-B); crime de extorsão (art. 158, CPB) e crime de concorrência desleal do artigo 195, inciso XII, da Lei nº 9.279/1996.

Como se trata de um crime sem fronteira, as medidas de enfrentamento vêm de países interessados no combate e prevenção de ilícitos, como Estados Unidos da América e Comunidade Européia.

Na Europa, inclusive, foi criado o NMR (No More Ransom), que é um sistema que auxilia as vítimas de *ransomware* a recuperar o acesso a seus dados sem necessidade de pagamento do resgate[16].

Em reunião ocorrida em outubro de 2021, convocada pela Casa Branca[17], 31 países, dentre eles o Brasil, comprometeram-se a adotar medidas para combater os ataques cibernéticos, incluindo a adoção de medidas contra a prática de lavagem de dinheiro e favoráveis à colaboração para investigações. A Conferência global[18] contra *Ransomware* estabeleceu quatro objetivos: melhorar a detecção desses crimes cibernéticos, aumentar a resiliência de redes e empresas públicas e privadas

---

14 Disponível em https://www.moneytimes.com.br/fabricio-alexandre-qual-e-a-relacao-entre-o-bitcoin-e-adeep-web/ (acesso em 18 de abril de 2022).

15 Disponível em https://assets.sophos.com/X24WTUEQ/at/hr6gj5b5v8btxpq68xqh34/sophos-it-security-team2021-beyond.pdf (acesso em 18 de abril de 2022).

16 Disponível em https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-andprevention-guides/no-more-ransom-do-you-need-help-unlocking-your-digital-life (acesso em 18 de abril de 2022). 17

Disponível em https://www.convergenciadigital.com.br/Seguranca/Brasil-participa-de-conferencia-globalcontra-ransomware-na-Casa-Branca-58431.html?UserActiveTemplate=mobile (acesso em 18 de abril de 2022). 18

Id.

a ataques, acabar com a impunidade que protege as *criptomoedas*, normalmente usadas para o pagamento de resgates e aumentar a cooperação internacional no combate ao cibercrime.

Ressalte-se que está em trâmite no Congresso Nacional o Projeto de Lei nº 3.825/2019 que cria regras para o mercado nacional de criptomoedas.

A participação brasileira serve de alento para que os órgãos de controle, combate e repressão ao ilícito, notadamente o Ministério Público, possam angariar instrumentos eficazes de atuação, além da maior facilidade de acesso à cooperação internacional.

Segundo especialistas, na atuação individual, uma das saídas para tentar evitar os ataques ou minimizar os danos é realizar *backup's*, instalar antivírus e evitar o acesso a ícones suspeitos.

LEI GERAL DE PROTEÇÃO DE DADOS

Sob o aspecto legal, no Brasil, os ataques *ransomware* precisam ser compreendidos à luz da Lei nº 13.709, de 14 de agosto de 2018, mais conhecida como Lei Geral de Proteção de Dados Pessoais ("LGPD"), que entrou em vigor em apenas 2 (dois) anos após a sua publicação, ao menos em relação à maior parte de seus dispositivos.

A LGPD dispõe sobre o tratamento de dados pessoais, sobretudo nos meios digitais, visando à proteção de direitos fundamentais, notadamente o direito à privacidade.

Essa Lei traz importantes dispositivos conceituais, necessários para a compreensão de suas normas, definindo, por exemplo, que "titular" é a *pessoa natural a quem se referem os dados pessoais que são objeto de tratamento*; "controlador" é a pessoa *a quem competem as decisões referentes ao tratamento de dados pessoais*; "operador" é a pessoa *que realiza o tratamento de dados pessoais em nome do controlador*; e "autoridade nacional" é o *órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional* (art. 5º, incs. V, VI, VII e XIX).

A LGPD contempla uma série de normas que impõem as obrigações a que estão sujeitas as pessoas responsáveis por lidar com dados pessoas de seus clientes e de terceiros, estabelecendo, ainda, um rigoroso regime de responsabilização administrativa e civil como consequência do descumprimento daquelas obrigações.

Nesse sentido, por exemplo, há expressa norma incumbindo ao controlador o dever de comunicar à autoridade nacional e aos titulares dos dados eventual incidente de segurança – a exemplo de ataques *ransomware* - que possa acarretar riscos ou danos relevantes a estes (art. 48), medida importante para alertar as vítimas indiretas dos riscos a que estão sujeitas, permitindo-lhes a adoção de medidas imediatas para mitigar os riscos de sofrer danos materiais e imateriais.

Sem prejuízo disso, a lei atribui ao "controlador" e ao "operador" a obrigação de reparar os danos causados pelo *exercício de atividade de tratamento de dados pessoais em violação à legislação de proteção de dados pessoais*, com possibilidade de inversão do ônus da prova a favor do titular dos dados, sempre que *for verossímil a alegação*, *houver hipossuficiência para fins de produção de prova* ou *quando a produção de prova pelo titular resultar-lhe excessivamente onerosa* (art. 42, *caput* e §2º).

Por outro lado, a LGPD afasta a possibilidade de responsabilização dos agentes de tratamento de dados pessoais quando provarem, alternativamente: a) *que não realizaram o tratamento de dados pessoais*; b) *que não houve violação à legislação de proteção de dados*; ou c) *que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro* (art. 43). Esta última hipótese tem especial relevância no debate acerca dos ataques *ransomware* que tem vitimizado empresas de forma crescente nos últimos anos, pois a definição da existência de "culpa exclusiva" de terceiro passará pela análise das medidas adotadas pelas empresas para proteger os dados pessoas sob sua responsabilidade, diminuindo as chances de êxito de ações criminosas virtuais praticadas por terceiros, a exemplo dos ataques *ransomware*.

Nesse diapasão, o art. 44 da LGPD estabelece que o tratamento de dados pessoais será *irregular* quando deixar de observar a legislação vigente ou, alternativamente, quando *não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes*, notadamente *o modo pelo qual é*

realizado, *o resultado e os riscos que razoavelmente dele se esperam* e *as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado*.

Como se vê, a lei se vale de diversos conceitos jurídicos indeterminados ao tratar do regime de responsabilização, deixando margem ampla para a discricionariedade motivada do juiz no julgamento dos casos concretos.

Esse espaço discricionário tende a ser reduzido pela implementação de *padrões técnicos mínimos* para a adoção das medidas de segurança dos dados, atividade essa reservada ao órgão federal criado pela própria LGDP, designado de Autoridade Nacional de Proteção de Dados (art. 46, §1º c/c arts. 55-A a 55-L). A propósito, a autoridade nacional vem editando atos normativos para regulamentar a LGPD, medida essencial para que a aplicação da lei ocorra com respeito à segurança jurídica[14].

Concomitantemente à obrigação de reparar danos causados a seus clientes e a terceiros (responsabilidade civil), a LGPD estabelece um sistema de responsabilização administrativa que alcança os agentes de tratamento de dados, em razão de infrações às normas dessa lei.

As sanções administrativas que a autoridade nacional pode aplicar, levando em conta os critérios legais estabelecidos e a regulamentação infralegal a ser editada, incluem a "advertência", com indicação de prazo para adoção de medidas corretivas, multa de até 2% (dois por cento) do faturamento da empresa no seu último exercício, limitada a R$ 50.000.000,00 (cinquenta milhões de reais) por infração, proibição do exercício de atividades relacionadas a tratamento de dados, dentre outras (art. 52).

Embora esse regramento fosse necessário para estabelecer, de forma clara, as obrigações das pessoas (físicas e jurídicas) que lidam com dados pessoais de seus clientes e terceiros, assim como as consequências pelo descumprimento dessas obrigações, fato é que a edição da LGPD tem sido apontada como um fator de incremento de ataques ransomware contra as empresas.

Atualmente, os criminosos por trás desses ataques não têm se limitado a criptografar os arquivos das empresas, mas buscam também extrair os dados da organização, ameaçando os gestores da entidade vítima de vazarem o conteúdo dos arquivos, caso não seja feito o pagamento do valor de resgate[15].

---

[14] Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes, acesso em 20/04/2022.

[15] Disponível em: https://valor.globo.com/legislacao/noticia/2021/10/04/ransomware-e-algpd.ghtml, acesso em 20/04/2022.

Actualmente, los criminales detrás de estos ataques no se han limitado a cifrar los archivos de las empresas, sino que buscan también extraer los datos de la organización, amenazando a los gestores de la entidad víctima con filtrar el contenido de los archivos, si no se efectúa el pago del valor de rescate[15].

CONCLUSÃO

O objetivo do presente artigo foi chamar a atenção para evolução tecnológica e como a atuação ilícita/criminal via internet, especialmente em relação ao *Ramsomware*, pode causar graves prejuízos financeiros e sociais, bem como sobre a importância do aperfeiçoamento e especialização da atuação do Ministério Público a fim de cumprir seu mister constitucional.

REFERÊNCIAS

BRASIL, Lei n 13.709, de 14 de agosto de 2018.

Disponível em https://valor.globo.com/legislacao/noticia/2021/10/04/ransomware-e-a- lgpd.ghtml, Felipe Palhares, acesso em 20/04/2022; https://www.gov.br/anpd/pt-br/documentos-e-publicacoes, acesso em 20/04/2022; https://g1.globo.com/politica/noticia/2020/11/04/stj-aciona-pf-para-apurar-possivelataque-de-hackers-ao-sistema-do-tribunal.ghtml (acesso em 18 de abril de 2022); https://www.tecmundo.com.br/seguranca/206233-ataque-hacker-ter-atingido-stj-pf-investiga.htm (acesso em 18 de abril de 2022); https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack (acesso em 18 de abril de 2022); https://assets.sophos.com/X24WTUEQ/at/hr6gj5b5v8btxpq68xqh34/sophos-itsecurity-team-2021-beyond.pdf (acesso em 18 de abril de 2022); https://www.moneytimes.com.br/fabricio-alexandre-qual-e-a-relacao-entre-o-bitcoin-e-a-deep-web/ (acesso em 18 de abril de 2022); https://www.europol.europa.eu/operations-services-and-innovation/publicawareness-and-prevention-guides/no-more-ransom-do-you-need-help-unlocking-your-digital-life (acesso em 18 de abril de 2022); https://www.convergenciadigital.com.br/Seguranca/Brasil-participa-de-conferenciaglobal-contra-ransomware-na-Casa-Branca-58431.html?

UserActiveTemplate=mobile (acesso em 18 de abril de 2022); https://cointelegraph.com.br/news/chainalysis-only1-of-1-trillion-transacted-in-crypto-in-2019-was-illicit (acesso em 18 de abril de 2022) e www1.folha.uol.com.br (acesso em 19/04/2022).

LISKA, Allan; GALLO, Timothy. Ransomware (Defendendo-se da Extorsão Digital). 1ª ed. São Paulo: Novatec Editora Ltda., 2017.

INTRODUCCIÓN

La Fiscalía posee atribuciones previstas tanto en la Constitución Federal como en la legislación infraconstitucional para la defensa del orden jurídico, régimen democrático y derechos sociales e individuales indisponibles.

La actuación institucional está marcada, no raras veces, por la transdisciplinariedad, dado el entrelazamiento de temas y materias en el ejercicio, en concreto, de las actividades.

Como titular de la acción penal, compete a la Fiscalía la promoción de todos los actos necesarios para el fiel cumplimiento de su múnus, destacadamente aquellos relacionados a la fase de investigación.

Si, en los crímenes más comúnmente practicados, existe evidente *expertise* de las policías, civil y federal, para su elucidación, la realidad se muestra distinta cuando la conducta involucra aspectos peculiares, tales como aquella que ofende el medio ambiente, anciano, mujer, niño y adolescente, patrimonio público y cultural, consumidor, entre otros intereses difusos.

En este escenario específico, la Fiscalía se hace protagonista en razón, sobre todo, del modelo adoptado, *interna corporis*, para distribución de sus atribuciones, de modo que la defensa de los derechos difusos, de forma especializada y sistematizada, todavía innovada en determinados órganos e instituciones, es promovida por el *Parquet* desde la promulgación de la Constitución de 1988 e incluso antes de eso, haya visto la vigencia de la Ley de Acción Civil Pública (7.347/85).

Un buen ejemplo de la actuación especializada con elementos de la transdisciplinariedad está en la actuación junto a los Juzgados de Derecho Empresarial donde, a principio o en la mayor parte de las veces, la actividad se relaciona al acompañamiento de procesos de quiebra y de recuperación judicial.

Los procedimientos de quiebra y de recuperación judicial implican, sin embargo, debates no solo de Derecho Empresarial, sino también en gran parte, su repercusión criminal y civil, propiamente dichas, ante la posibilidad de prácticas ilícitas anteriores, tales como competencia desleal, lavado de dinero, lesiones a los consumidores, fraude a los acreedores, entre otros.

En este sesgo, la atención de la Fiscalía no se concentra en aspectos meramente formales, exigiéndose, al contrario, amplia indagación acerca del panorama fático-jurídico que haya precedido al procedimiento de quiebra y de

recuperación judicial, con el fin de impedir el uso indebido de tales institutos jurídicos.

La reciente operación "Lava Jato", a modo de ejemplo, fomentó diversos procedimientos de tal naturaleza, de modo a embarajar discusiones criminales, empresariales y políticas e imponer una mirada cautelosa de aquel que, a principio, sería un mero fiscal del orden jurídico.

En este contexto, se denota que Fiscales de Justicia deben conocer no solo los conceptos técnicos del Derecho Empresarial, sino, precipuamente, el propio modelo de funcionamiento de cada empresa, su realidad comercial y contable, para que pueda ejercer con seguridad sus atribuciones a fin de ver distorsiones de gestión y eventuales ilicitudes practicadas por socios, gestores o terceros.

RANSOMWARE e BITCOINS

Una práctica que ha generado innegable malestar es el *Ransomware*, popularmente conocido como secuestro de datos o secuestro digital.

En realidad, se trata de un *malware* (software malicioso) que cifra archivos y documentos, locales y de red, impidiendo su acceso con el objetivo de obtener una ventaja ilícita.

En un panorama histórico sobre el tema es importante resaltar que Internet surgió en los Estados Unidos de América en 1969, pero hasta entonces era volcada exclusivamente para la defensa norteamericana en la fase de la Guerra Fría, Su objetivo era garantizar la comunicación entre científicos y militares durante los bombardeos.

En los Estados Unidos el uso comercial de Internet fue autorizado desde 1987 y en 1989 se produjo el primer ataque documentado de *Ransomware*.

Este primer ataque fue realizado vía disquetes distribuidos por "*Joseph Popp, PhD, un investigador del SIDA, alegando que los discos contenían un programa que analizaba el riesgo de un individuo de adquirir SIDA por medio de cuestionario. Sin embargo, el disco también contenía un programa de malware que inicialmente permaneció inactivo en las computadoras, activándose solo después de que una computadora fuera conectada 90 veces. Después de que se alcanzó el límite de 90 inicializaciones, el malware exhibió un mensaje exigiendo un pago de $ 189 y otros $*

378 por un alquiler de software. Este ataque de ransomware se conoció como el ***Trojan*** *del* ***SIDA****, o PC Cyborg*."

Los principales ataques de *Ransomware* fueron: *WannaCry* en 2017; *BadRabbit*; *Cerber*; *Darkside*; *Crysis*; *Locky*; *Jigsaw*; *Petya*; *Goldeneye*; *Reveton*; *Maze ransomware*.

Esta especie de secuestro de datos puede tener como víctima a personas físicas, jurídicas e incluso instituciones públicas, siendo que Brasil está en la lista de los diez países con mayor número de víctimas del *Ransomware* y los principales casos fueron: JBS empresa distribuidora de alimentos; Lojas Renner; Superior Tribunal de Justicia, Ministerio de Salud y el Tesoro Nacional.

Los practicantes de tal ilícito pueden tener objetivos diversos. En 2020, el caso del Superior Tribunal de Justiça[16] que generó la suspensión de plazos y actividades internas dada su magnitud, debido a haber sido cifrada toda la base de datos, *backups*, dejando el sistema inaccesible para el público interno y externo[17].

Las empresas privadas, en la mayoría de los casos, se convierten en el objetivo preferido, ya sea por la mayor facilidad de pago de los rescates o incluso por prácticas competitivas ilícitas.

En otro caso emblemático, ocurrido en mayo de 2021, Colonial Pipeline, una empresa estadounidense activa en el ramo de oleoductos y situada en Houston, Texas, sufrió un *cyberattack* que impactó toda su red de informática, lo que fue considerado el mayor ataque ocurrido en aquel país, obligando a la empresa víctima a efectuar el pago del rescate en *criptomoneda* (*bitcoin*)[18].

La intervención de la Fiscalía en la lucha y prevención de lo ilícito impone aún el conocimiento acerca del mercado de las *criptomonedas*, especialmente el *bitcoin*, en razón de ser el tipo de rescate comúnmente exigido.

Operaciones ilícitas de criptomonedas, en especial *bitcoins*, ocurren en la llamada "deep web" o "dark web", término creado por Mike Bergman, en 2000[19], ante la fragilidad de mecanismos de control y dificultad de rastreo.

El aumento progresivo de casos ya fue objeto de investigación, realizada por Vanson Bourne[15], lo que solo confirma la actualidad del tema.

---

[16] Disponible en https://g1.globo.com/politica/noticia/2020/11/04/stj-aciona-pf-para-apurar-possivel-ataquede-hackers-ao-sistema-do-tribunal.ghtml (acceso el 18 de abril de 2022).

[17] Disponible en https://g1.globo.com/politica/noticia/2020/11/04/stj-aciona-pf-para-apurar-possivel-ataquede-hackers-ao-sistema-do-tribunal.ghtml (acceso el 18 de abril de 2022).

[18] https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack (acceso el 18 de abril de 2022).

En el derecho brasileño la práctica encuentra previsión típica en los artículos 154-A, 154-B, 171, párrafos 2º y 2º y 266, del Código Penal Brasileño.

Se considera, aún, sobre la viabilidad de imputación de hurto calificado (art. 155, § 4º-B); crimen de extorsión (art. 158, CPB) y crimen de competencia desleal del artículo 195, inciso XII, de la Ley nº 9.279/1996.

Como se trata de un crimen sin fronteras, las medidas de enfrentamiento vienen de países interesados en el combate y prevención de ilícitos, como los Estados Unidos de América y la Comunidad Europea.

En Europa, incluso, se ha creado el NMR (No More Ransom), que es un sistema que ayuda a las víctimas de *ransomware* a recuperar el acceso a sus datos sin necesidad de pago del resgate[16].

En una reunión ocurrida en octubre de 2021, convocada por la Casa Blanca[17], 31 países, entre ellos Brasil, se comprometieron a adoptar medidas para combatir los ataques cibernéticos, incluyendo la adopción de medidas contra la práctica de lavado de dinero y favorables a la colaboración para investigaciones. La Conferencia global[18] contra *Ransomware* estableció cuatro objetivos: mejorar la detección de estos delitos cibernéticos, aumentar la resiliencia de las redes y de las empresas públicas y privadas a ataques, acabar con la impunidad que protege las *criptomonedas*, normalmente utilizadas para el pago de rescates y aumentar la cooperación internacional en la lucha contra el cibercrimen.

Cabe señalar que está en trámite en el Congreso Nacional el Proyecto de Ley nº 3.825/2019 que crea reglas para el mercado nacional de criptomonedas.

La participación brasileña sirve de aliento para que los órganos de control, combate y represión a lo ilícito, especialmente la Fiscalía, puedan obtener instrumentos eficaces de actuación, además de una mayor facilidad de acceso a la cooperación internacional.

Según los expertos, en la actuación individual, una de las salidas para intentar evitar los ataques o minimizar los daños es realizar *backup's*, instalar antivirus y evitar el acceso a iconos sospechosos.

14

Disponible en https://www.moneytimes.com.br/fabricio-alexandre-qual-e-a-relacao-entre-o-bitcoin-e-adeep-web/ (acceso el 18 de abril de 2022).

15

Disponible en https://assets.sophos.com/X24WTUEQ/at/hr6gj5b5v8btxpq68xqh34/sophos-it-security-team2021-beyond.pdf (acceso el 18 de abril de 2022).

16 Disponible en https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-andprevention-guides/no-more-ransom-do-you-need-help-unlocking-your-digital-life (acceso el 18 de abril de 2022).

17 Disponible en https://www.convergenciadigital.com.br/Seguranca/Brasil-participa-de-conferencia-globalcontra-ransomware-na-Casa-Branca-58431.html?UserActiveTemplate=mobile (acceso el 18 de abril de 2022).

18 Id.

LEY GENERAL DE PROTECCIÓN DE DATOS

Bajo el aspecto legal, en Brasil, los ataques *ransomware* necesitan ser comprendidos a la luz de la Ley nº 13.709, del 14 de agosto de 2018, más conocida como Ley General de Protección de Datos Personales ("LGPD"), que entró en vigor en solo 2 (dos) años tras su publicación, al menos en relación con la mayoría de sus dispositivos.

La LGPD dispone sobre el tratamiento de datos personales, sobre todo en los medios digitales, buscando la protección de los derechos fundamentales, en particular el derecho a la privacidad.

Esta Ley trae importantes dispositivos conceptuales, necesarios para la comprensión de sus normas, definiendo, por ejemplo, que "titular" es *la persona natural a quien se refieren los datos personales que son objeto de tratamiento*; "controlador" es *la persona a la que competen las decisiones relativas al tratamiento de datos personales*; "operador" es la persona *que realiza el tratamiento de datos personales en nombre del controlador*; y "autoridad nacional" es el *órgano de la administración pública responsable de velar, implementar y fiscalizar el cumplimiento de esta Ley en todo el territorio nacional* (art. 5º, incs. V, VI, VII y XIX).

La LGPD contempla una serie de normas que imponen las obligaciones a que están sujetas las personas responsables de tratar con los datos personales de sus clientes y de terceros, estableciendo, además, un estricto régimen de responsabilidad administrativa y civil como consecuencia del incumplimiento de dichas obligaciones.

En este sentido, por ejemplo, existe una regla expresa incumbiendo al controlador el deber de comunicar a la autoridad nacional y a los titulares de los datos cualquier incidente de seguridad - a ejemplo de ataques *ransomware* - que pueda acarrear riesgos o daños relevantes a estos (art. 48), medida importante para alertar a las víctimas indirectas de los riesgos a los que están expuestas, permitiéndoles adoptar medidas inmediatas para mitigar los riesgos de sufrir daños materiales e inmateriales.

Sin perjuicio de esto, la ley atribuye al "controlador" y al "operador" la obligación de reparar los daños causados por el *ejercicio de actividad de tratamiento de datos personales en violación de la legislación de protección de datos personales*, con posibilidad de invertir la carga de la prueba en favor del titular de los datos, siempre que *sea verosímil la alegación, haya insuficiencia para fines de producción de pruebas o cuando la producción de pruebas por el titular le resulte excesivamente onerosa* (art. 42, caput y §2º).

Por otra parte, la LGPD rechaza la posibilidad de responsabilizar a los agentes de tratamiento de datos personales cuando demuestren, alternativamente: *a) que no realizaron el tratamiento de datos personales*; *b) que no hubo violación de la legislación de protección de datos*; o *c) que el daño es consecuencia de la culpa exclusiva del titular de los datos o de un tercero* (art. 43). Esta última hipótesis tiene especial relevancia en el debate acerca de los ataques *ransomware* que han victimizado empresas de forma creciente en los últimos años, pues la definición de la existencia de "culpa exclusiva" de terceros pasará por el análisis de las medidas adoptadas por las empresas para proteger los datos de personas bajo su responsabilidad, disminuyendo las posibilidades de éxito de acciones criminales virtuales practicadas por terceros, a ejemplo de los ataques *ransomware.*

En este contexto, el art. 44 de la LGPD establece que el tratamiento de datos personales será *irregular* cuando deje de observar la legislación vigente o, alternativamente, cuando *no proporcione la seguridad que el interesado puede esperar, teniendo en cuenta las circunstancias relevantes, especialmente el modo en que se lleva a cabo, el resultado y los riesgos que razonablemente se esperan de él y las técnicas de tratamiento de datos personales disponibles en el momento en que se realizó.*

Como se ve, la ley se vale de diversos conceptos jurídicos indeterminados al tratar del régimen de responsabilización, dejando amplio margen para la discrecionalidad motivada del juez en el juicio de los casos concretos.

Este espacio discrecional tiende a ser reducido por la implementación de *estándares técnicos mínimos* para la adopción de las medidas de seguridad de los datos, actividad que está reservada al órgano federal creado por la propia LGDP, designado como Autoridad Nacional de Protección de Datos (art. 46, §1º c/c arts. 55-A a 55-L). A propósito, la autoridad nacional viene editando actos normativos para regular la LGPD, medida esencial para que la aplicación de la ley ocurra con respecto a la seguridad jurídica[14].

Simultáneamente a la obligación de reparar daños causados a sus clientes y a terceros (responsabilidad civil), la LGPD establece un sistema de responsabilidad administrativa que alcanza a los agentes de tratamiento de datos, en razón de infracciones a las normas de dicha ley.

Las sanciones administrativas que la autoridad nacional puede aplicar, teniendo en cuenta los criterios legales establecidos y la normativa infralegal a editarse, incluyen la "advertencia", con indicación de plazo para la adopción de medidas correctivas, multa de hasta el 2% (dos por ciento) de la facturación de la empresa en su último ejercicio, limitada a R$ 50.000.000,00 (cincuenta millones de reales) por infracción, prohibición del ejercicio de actividades relacionadas con el tratamiento de datos, entre otras (art. 52).

Si bien esta normativa era necesaria para establecer de forma clara las obligaciones de las personas (físicas y jurídicas) que tratan con datos personales de sus clientes y terceros, así como las consecuencias del incumplimiento de dichas obligaciones, lo cierto es que la edición de la LGPD ha sido designada como un factor en el aumento de los ataques de *ransomware* contra las empresas.

CONCLUSIÓN

El objetivo del presente artículo fue llamar la atención sobre la evolución tecnológica y cómo la actuación ilícita/criminal vía internet, especialmente en relación con *Ramsomware*, puede causar graves perjuicios financieros y sociales, así como sobre la importancia del perfeccionamiento y especialización de la actuación de la Fiscalía a fin de cumplir su misión constitucional.

REFERENCIAS

BRASIL, Lei n 13.709, de 14 de agosto de 2018.

Disponible en https://valor.globo.com/legislacao/noticia/2021/10/04/ransomware-e-a- lgpd.ghtml, Felipe Palhares, acceso el 20/04/2022; chttps://www.gov.br/anpd/pt-br/documentos-e-publicacoes, acceso el 20/04/2022; https://g1.globo.com/politica/noticia/2020/11/04/stj-aciona-pf-para-apurar-possivelataque-de-hackers-ao-sistema-do-tribunal.ghtml (acceso el 18 de abril de 2022); https://www.tecmundo.com.br/seguranca/206233-ataque-hacker-ter-atingido-stj-pf-investiga.htm (acceso el 18 de abril de 2022); https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack (acceso el 18 de abril de 2022); https://assets.sophos.com/X24WTUEQ/at/hr6gj5b5v8btxpq68xqh34/sophos-itsecurity-team-2021-beyond.pdf (acceso eel 18 de abril de 2022); https://www.moneytimes.com.br/fabricio-alexandre-qual-e-a-relacao-entre-o-bitcoin-e-a-deep-web/ (acceso el 18 de abril de 2022); https://www.europol.europa.eu/operations-services-and-innovation/publicawareness-and-prevention-guides/no-more-ransom-do-you-need-help-unlocking-your-digital-life (acceso el 18 de abril de 2022); https://www.convergenciadigital.com.br/Seguranca/Brasil-participa-de-conferenciaglobal-contra-ransomware-na-Casa-Branca-58431.html?UserActiveTemplate=mobile (acceso eel 18 de abril de 2022); https://cointelegraph.com.br/news/chainalysis-only1-of-1-trillion-transacted-in-crypto-in-2019-was-illicit (acceso eel 18 de abril de 2022) y www1.folha.uol.com.br (acceso el 19/04/2022).

LISKA, Allan; GALLO, Timothy. Ransomware (Defendendo-se da Extorsão Digital). 1ª ed. São Paulo: Novatec Editora Ltda., 2017.