Claudio Joel Brito Lóssio

O DIREITO E O CIBERESPAÇO

2ª edição revista e atualizada

DESTAQUES:

- Direito dos Ciborgues
- Computação Cognitiva e o Direito
- *Blockchain* e o *Compliance*
- Ciberataques e Ciberdefesa
- Cibernética e a Juscibernética
- Ciberterrorismo e *Hacking*
- Ciclo da Resiliência no Ciberespaço
- Globalização e a *Cyber-Drittwirkung*
- Direito ao Esquecimento e a *Blockchain*
- Direitos Humanos e o Monitoramento das Comunicações
- Doutrina Jurídica em Direito Digital
- Indústria 4.0 e Sociedade 5.0
- Proteção de Dados Pessoais
- Resolução Alternativa de Litígios em Domínios
- Soberania e a Teoria Pentadimensional do Direito

2024

EDITORA *Jus*PODIVM

www.editorajuspodivm.com.br

7

O *Compliance* e o Ciberterrorismo

O avanço da tecnologia e da informática são os motores da evolução social, criando, assim, um modelo, a sociedade digital. O ciberespaço é necessário para a existência dessa nova sociedade, assim como a internet é necessária para que exista o ciberespaço.

O desenvolvimento desta escrita foi incentivado pela quantidade de empresas e pessoas que tiveram suas informações atacadas por *ransomware* em todo o mundo. Ataques que fizeram empresas, bancos, governos e hospitais pararem ou violaram o seu padrão de funcionamento em vários locais do mundo, seja no Brasil ou na Europa, por exemplo. Também incentivado pelo novo Regulamento Geral da Proteção de Dados da Europa em sua necessidade de aplicação do trabalho de conformidade em empresas da União Europeia que armazenam dados pessoais, como também o compliance em proteção de dados pode ser determinante e condicionante para que essas organizações estejam no mercado.

Esse trabalho de conformidade é também denominado trabalho de *compliance* e quando se trata em promover tal segurança na seara da TI digital, então é denominado *compliance* digital, que está voltado para garantir a segurança tanto nas empresas quanto para as pessoas, por meio de políticas e normas internas ou externas.

No primeiro momento serão abordados os protagonistas e alguns elementos necessários para entender melhor esta escri-ta. Os principais protagonistas entre os criminosos, os comba-

tentes e as vítimas são respectivamente os *hackers*, mais precisamente os *black hats*, que desviam seus conhecimentos para a prática dos delitos, os profissionais da segurança da informação serão os que promoverão a segurança dos sistemas, assim como farão parte da equipe do *compliance* digital, e, por último, como vítimas, estão os usuários, que são as pessoas comuns com conhecimento básico de informática, que normalmente têm seus dispositivos invadidos devido sua imperícia ou imprudência.

O ciberterrorismo será apresentado no subtópico segundo, mostrando que os *hackers* buscam aterrorizar o mundo através de ataques por meio do *ransomware*, disponibilizando informações particulares e ferindo a ordem pública, sendo tal crime considerado ato terrorista tanto no Código Penal brasileiro quanto na Convenção de Budapeste.

O terceiro subtópico será o resultado da investigação, explicando cada ato feito pelo *ransomware*, desde a sua confecção até a devolução ou não das informações sequestradas pela sua encriptação. Cada passo do *ransomware* será relacionado com o Código Penal Brasileiro, assim como com a Convenção de Budapeste e em alguns casos até será apresentado diante das leis de combate ao terrorismo, tanto brasileira quanto portuguesa.

Os passos que serão mostrados serão a partir do planejamento e desenvolvimento do seu código malicioso; o ponto em que esse código fisgará o usuário em um e-mail falso; a violação de segurança e acesso ilegal ao computador do usuário; a encriptação dos dados, que é a codificação destes, ferindo o princípio da disponibilidade da segurança da informação; o pagamento para resgatar as informações e por último o ato da liberação ou não da chave de segurança necessária para decriptação dos arquivos.

No quarto subtópico será apresentado brevemente o trabalho de *compliance* por meio de medidas que poderão combater o ciberterrorismo, visto que, se forem seguidas, não ocorrerá a incitação do *ransomware* por e-mail. Possuir o conhecimento na tecnologia é um fator determinante para conseguir combater os crimes atuais, os cibernéticos. Assim como as boas práticas diante do uso da informática podem ser as maiores ferramentas contra o *ransomware*, códigos maliciosos, como vários outros *malwares*.

Por último, algumas notícias sobre ataques pelo *ransomware* e como este parou o mundo. Para tal desenvolvimento foram utilizados os seguintes métodos de abordagem: dedutivo e dialético. No que se refere ao procedimento, os métodos adotados serão: estudo de caso e comparativo. As técnicas de pesquisa utilizadas para confecção da dissertação serão a bibliográfica e documental.

Cabe ressaltar que o tema está relacionado com a Informática e o Direito, algumas das pesquisas serão feitas com o auxílio da internet para se obter acesso a documentos e livros eletrôni-cos que não possam ser adquiridos de forma física e/ou direta.

A seguir iniciaremos com os elementos informáticos que são necessários para o melhor entendimento no que se versa a sociedade digital, os protagonistas do ciberespaço e o *ransomware*.

7.1 A Sociedade Digital e o *Ransomware*

O uso de novas tecnologias na sociedade traz facilidades e possibilidades antes inimagináveis, auxiliando na área da saúde, do direito, das comunicações e das tecnologias da informação, por exemplo, revolucionando e proporcionando as informações automáticas nesses diversos processos por meio da informática.

Dentre as tecnologias, indiscutivelmente as que mais se destacam são o computador e a internet. Pois é através necessariamente da existência destes que os processos automáticos das demais tecnologias fluem, como a inteligência artificial e a *blockchain*. É graças à internet que as barreiras geográficas foram quebradas, proporcionando a troca de cultura e conhecimento, trazendo assim para a sociedade uma nova forma de se relacionar.[1]

É importante ressaltar que o ciberespaço e a sociedade digital são duas coisas distintas, porém, são totalmente interligadas. O ciberespaço é um local onde há a troca de conhecimentos e de informações, composto por estruturas de rede física e lógi-ca, assim como as pessoas que as compõe, as cyberpersonas. Es-

1. POLICARPO, Poliana; BENNARD, Edna. *Cibercrimes na E-Democracia*. 2. ed. Belo Horizonte: Editora D'Plácido, 2017. p. 50.

sas cyberpersonas formam a sociedade conectada, compondo o ciberespaço, onde, através da internet, as pessoas se conectam e vivem um tipo de relação, produzindo conteúdo e trocando informações.[2]

A sociedade digital, também denominada sociedade em rede, é uma evolução do status *a quo* da sociedade em que vivemos para o status *ad quem*, criando um modelo social digital, em que há uma união completa do mundo real com o mundo digital, visto que o ocorrido no ambiente cibernético afeta até mais as pessoas no ambiente real, como no caso de sofrer uma difamação por meio de uma rede social.[3]

A sociedade digital é resultado do impulso do desenvolvimento tecnológico, sendo necessária uma imersão de todos diante do conhecimento tecnológico proporcionado pela informática.[4] Seria uma parte da sociedade da informação.

Olhando por uma perspectiva evolutiva, a popularização da informática na utilização dos microcomputadores foi o primeiro passo da revolução computacional, o segundo passo da veio com o surgimento do uso da internet e com a popularização das redes sociais, da comunicação em massa. O terceiro e atual passo dessa evolução dos computadores surge com a utilização de ferramentas que buscam a segurança e a confiança de qualquer informação, promovendo assim o *compliance* e a *accountability* em qualquer trabalho, assim como proposto pelo Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia[5], sobre o qual praticamente todas as empresas presentes na União Europeia deverão ter um trabalho de conformidade, para as informações em acervo de dados pessoais tanto físico quanto digital.

Mesmo o RGPD sendo da Europa, influenciará todo o mundo, visto que os dados presentes na internet comumente não

2. Idem, Op. cit., p. 49.
3. SAKAMOTO, Leonardo. *O que aprendi sendo xingado na internet*. São Paulo: Leya, 2016.
4. PINHEIRO, Patrícia Peck. *#DireitoDigital*. 6. ed. São Paulo: Saraiva, 2016. p. 67.
5. DATEN, Shutz. *Regulamento Geral sobre a Proteção de Dados da União Europeia*. 2017. Disponível em: http://www.privacy-regulation.eu/pt/. Acesso em: 13 dez. 2017.

seguem o princípio da territorialidade. A aplicabilidade extraterritorial do RGPD será a todas as pessoas que tratem dados de europeus. Esse regulamento é claro quando versa que o importante é garantir a proteção dos dados pessoais de todos os cidadãos europeus, mesmo estes estando fora do continente europeu[6]. Ainda assim, seria de supra importância de uma legiferação específica no Brasil, visto que essa seria de suma importância para o desenvolvimento econômico e tecnológico diante da promoção de segurança jurídica, assim como garantindo o direito à proteção de dados pessoais, no caso da LGPD, e em âmbito constitucional, após positivada a Emenda Constitucio-nal 115, que inseriu "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".

Em busca de conceituar o que sejam essas expressões, *compliance* e *accountability*, o primeiro vem de conformidade, cumprimento, direito, regularidade, de buscar estar dentro do normativo legal e segundo a política interna da empresa[7]. Já *accountability* é a busca pela ética por meio da transparência do processo e procedimento da aplicação do trabalho de conformidade[8].

Para entendermos a relação do *compliance* diante do ciberterrorismo é necessário entender alguns elementos informáticos que constituem esse novo modelo social, como a *big data*, o *hacker*, a criptografia e o *ransomware*, entre outros, pois apenas diante de tais conceitos será proporcionada uma maior compreensão da temática.

---

6. SANTOS, Coriolano Aurélio de Almeida Camargo; CRESPO, Marcelo. "Como será o futuro dos negócios com a vigência do Regulamento Geral de Proteção de Dados Europeu?". Disponível em: http://www.migalhas.com.br/DireitoDigital/105,-MI266327,51045-Como+sera+o+futuro+dos+negocios+com+a+vigencia+do+Regulamento+Geral. Acesso em: 13 dez. 2017.

7. NYMITY innovating Compliance – *A Structure Approach to Privacy Management*: Getting Started Manual. 2017. Disponível em: https://www.nymity.com/data-privacy-resources/~/media/NymityAura/Resources/Privacy%20Management%20Primer/Structured-Privacy-Management_Getting-Started.pdf. Acesso em: 27 nov. 2017. p. 30.

8. NYMITY innovating Compliance. *A Structure Approach to Privacy Management*. Op. cit., p. 33.

Iniciaremos então o conceito das pessoas envolvidas no ambiente cibernético, como o usuário, os profissionais e os causadores do ciberterrorismo. Sem a existência destes, possivelmente a segurança da informação estaria desfavorecida, assim como os crimes digitais que dependem de um maior conhecimento inexistiriam, como sem o usuário a internet estaria obsoleta.

Iniciaremos pelo protagonista mais vulnerável dos que serão apresentados, o **usuário**. Os usuários são aqueles que acessam a internet e utilizam os recursos que por ela e por todos os provedores são oferecidos[9]. São todas as pessoas que de alguma maneira manuseiam a internet, diante da situação tratada, o ciberterrorismo.

Normalmente, a imprudência e a imperícia do usuário são os maiores causadores de problemas nos dispositivos informáticos que operam. Consequentemente proporcionam, pelo mau uso, seja do computador, do *smartphone*, das redes wi-fi, ou dos dispositivos de armazenamento, a brecha para que o dispositivo que estão operando seja violado, permitindo assim o acesso por terceiros mal-intencionados, os *hackers black hats*[10].

Os *hackers* são pessoas com grande conhecimento em códigos de computador, conseguindo encontrar falhas na proteção de sistemas informáticos. Mas o que os diferenciará entre si será o que farão ao descobrir tais falhas. Os *white hats* proporcionarão a segurança dos sistemas informáticos. Já os *black hats*, também denominados *crackers*, utilizarão tais falhas para invadir indevidamente o sistema informático[11].

Contudo é comum ver noticiários e comentários sempre atribuindo o termo *hacker* ao causador do delito cibernético, então, ao longo desta escrita, sempre que usarmos o termo *hacker*, estaremos nos referindo aos *hackers black hats*, os causado-

9. SANTOS, Antonio Jeová. *Dano moral indenizável*. 6. ed. Salvador: JusPodivm, 2016. p. 363.

10. TECHTARGET. *Hacker*. 2017. Disponível em: http://searchsecurity.techtarget.com/definition/hacker. Acesso em: 27 nov. 2017.

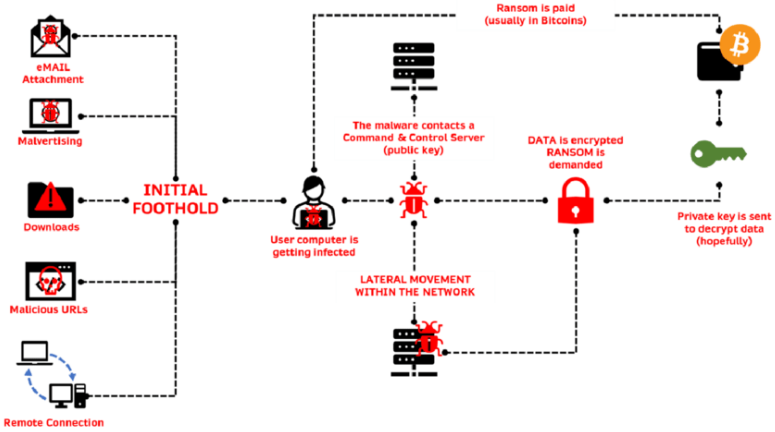
11. TECHTARGET. *Hacker*. Ibidem.

res dos cibercrimes, e o profissional de segurança da informação como protetor dos sistemas informáticos.

O correio eletrônico possibilita a comunicação entre usuários mediante o uso de uma conta exclusiva com identificação de usuário e senha. Os mais populares são Gmail, Hotmail e Yahoo[12]. O CERT.BR – Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil versa que o *ransomware* pode se propagar por vulnerabilidades nos sistemas segurança não atualizados e por código malicioso inserido em um e-mail, que será tratado nesta escrita.

> O *ransomware* pode se propagar de diversas formas, embora as mais comuns sejam: através de ***e-mails*** com o código malicioso em anexo ou que induzam o usuário a seguir um *link;* explorando **vulnerabilidades** em sistemas que não tenham recebido as devidas atualizações de segurança[13].

Figura 6 – Ransomware



Fonte: https://www.researchgate.net/profile/Sozon-Leventopoulos/publication/361925399/figure/fig4/AS:1176958918504451@1657620281898/How-ransomware-works-Source-Author.png

12. SANTOS, Antonio Jeová. *Dano moral indenizável*, p. 363.
13. CERT.br – *Cartilha de Segurança para Internet*: Ransomware. 2017. Disponível em: https://cartilha.cert.br/ransomware/. Acesso em: 14 dez. 2017.

É comum que o conteúdo malicioso do e-mail que será propagado pela internet esteja direcionado a pessoas ou a empresas que o *hacker* deseja atacar e por muitas vezes mesmo um conteúdo genérico atinge muitas pessoas em todo o mundo. Essa tática é um dos exemplos de engenharia social utilizada pelos *hackers* para conseguirem violar sistemas de segurança informáticos. A seguir conheceremos melhor o que é o *ransomware* e o que ele pode causar.

Segundo a IBM, o *ransomware*, como o próprio nome indica, é um *malware*[14] nefasto que retém os dados como um refém sequestrado, exigindo um pagamento para liberá-los como forma de resgate[15]. Ataques semelhantes às variantes *Petya* ou *WannaCry* são versões muito mais sofisticadas do *malware* típico. Eles aproveitam as explorações vazadas e usam criptografia forte.

Cleórbete Santo, versa que o *WannaCry*, supracitado, é uma praga do gênero *ransomware* é da espécie criptovírus[16]. Um *software* malicioso com direcionamento exclusivo para computadores que utilizam a plataforma Windows como sistema operacional, muito embora outros ransomware podem ser voltados para a plataforma Linux[17].

Normalmente um *hacker* disponibiliza *links* em sites inseguros, em aplicações piratas ou por e-mail, sobre o qual o usuário clica e o *ransomware* encontra uma brecha para seu dispositivo ser controlado remotamente e assim o invasor coleta seus dados sem autorização ou apenas os encripta com uma chave que só ele passa a saber[18].

---

14. *Malicious Software*, traduzindo, Software Malicioso.
15. IBM. "Are you safe from ransomware attacks?". Disponível em: https://www.ibm.com/security/ransomware. Acesso em: 27 nov. 2017.
16. SANTOS, Cleórbete. "Ataques do ransomware WannaCry e a Lei Carolina Dieckmann". Disponível em: https://cleorbete.jusbrasil.com.br/artigos/458420417/ataques-do-ransomware-wannacry-e-a-lei-carolina-dieckmann. Acesso em: 13 dez. 2017.
17. TECMUNDO. "Entenda o que é ransomware*:* o malware que sequestra computadores". Disponível em: https://www.tecmundo.com.br/seguranca-de-dados/116360-especialista-explica-crescimento-ransomware-brasil.htm. Acesso em: 13 dez. 2017.
18. Idem, Ibidem.

A encriptação é o meio mais seguro para se proporcionar a confidencialidade de informações e proteger arquivos, senhas e tudo o que for importante quando se fala em informação. Para efetuar a encriptação é exigida uma senha, denominada chave, pois só por meio desta será possível fazer a decriptação, assim tornando as informações acessíveis novamente[19].

Veremos a seguir a relação que o *ransomware* tem com o ciberterrorismo, verificando como esse *malware* pode afetar a vida de todos no mundo.

7.2 O *Ransomware* e o Ciberterrorismo

Algo se torna crime a partir do momento em que a sociedade decide punir algumas condutas específicas que julgam não serem compatíveis com a sociedade. Dessa forma, as situações definidas como crime variam em tempo e espaço, por exemplo, uma situação pode ser considerada crime em um determinado país, porém, em outro, essa conduta é completamente aceita. Ou seja, a ideia de crime não é uma ideia universal.[20]

O ciberterrorismo é um ato terrorista praticado no ciberespaço. Mas o que é o terrorismo?

A lei brasileira 13.260, de 16 de março de 2016, diz em seu art. 2º[21]:

> O terrorismo consiste na prática por um ou mais indivíduos dos atos previstos neste artigo, por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, quando cometidos com a **finalidade de provocar terror social ou generalizado**, expondo a perigo pessoa, **patrimônio, a paz pública ou a incolumidade pública**. (grifo nosso)

19. WYKES, Sean Michael. *Criptografia essencial: a jornada do criptógrafo*. Rio de Janeiro: Elsevier, 2016. p. 13.

20. POLICARPO, Poliana; BENNARD, Edna. *Cibercrimes na E-Democracia*. Op. cit., p. 107.

21. Lei 13.260/2016, de 16 de março. 2016. "Lei Antiterrorismo". Disponível em: http://www2.camara.leg.br/legin/fed/lei/2016/lei-13260-16-marco-2016-782561-publicacaooriginal-149752-pl.html. Acesso em: 6 dez. 2017.

Diante do artigo exposto acima, o ciberataque por ransomware é um ato terrorista, uma vez que o bloqueio das informações presentes nos computadores pessoais, empresariais e governamentais poderá, por exemplo, causar terror social ou generalizado, dano ao patrimônio e violação da paz pública.

Tal ato terrorista atinge as pessoas, sejam públicas ou particulares, não dotadas de conhecimento ou prudência suficiente para se protegerem diante da sociedade digital. Culturalmente não estamos habilitados e educados suficientemente para usufruir da internet com segurança[22], e normalmente estes são os mais atingidos por *malwares* e *hackers*.

A legislação de combate ao terrorismo portuguesa[23], em seu art. 4º, 2:

> Quem praticar crime de furto qualificado, roubo, **extorsão, burla informática** e nas comunicações, **falsidade informática**, ou falsificação de documento com vista ao cometimento dos factos previstos no n.º 1 do artigo 2.º, é punido com a pena correspondente ao crime praticado, agravada de um terço nos seus limites mínimo e máximo.

E em caso de organização terrorista[24], o art. 2º, 1, *d*:

> Considera-se grupo, organização ou associação terrorista todo o agrupamento de duas ou mais pessoas que, actuando concertadamente, visem prejudicar a integridade e a independência nacionais, **impedir, alterar ou subverter o funcionamento das instituições do Estado** previstas na Constituição, forçar a autoridade pública a praticar um acto, a abster-se de o praticar ou a tolerar que se pratique, ou ainda intimidar certas pessoas, grupos de pessoas ou a população em geral, mediante:
>
> d) Actos que destruam ou que **impossibilitem o funcionamento ou desviem dos seus fins normais, definitiva ou**

22. PINHEIRO, Patrícia Peck. *#DireitoDigital*. Ibidem.

23. Lei 52/2003, de 22 de Agosto. "Lei de Combate ao Terrorismo". Disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=119&tabela=leis. Acesso em: 6 dez. 2017.

24. Idem, Ibidem.

> **temporariamente, total ou parcialmente, meios ou vias de comunicação**, instalações de serviços públicos ou destinadas ao abastecimento e satisfação de necessidades vitais da população;

O ciberterrorismo por *ransomware* busca por meio do medo e do terror alcançar seus objetivos. Utiliza-se da encriptação das informações do lesado, ameaçando por meio de extorsão, com a finalidade de obter um pagamento de um valor para resgate das informações contidas no computador.

O ciberespaço tem se tornado uma arma poderosa para a prática dessas ações, promovendo o medo para a população, violando e invadindo sistemas governamentais, gerando o caos. Para isso, eles utilizam técnicas e softwares específicos além das técnicas físicas para danificar e violar sistemas[25], como, por exemplo, o *ransomware*.

Grande parte dos usuários não sabem a dimensão que possui a internet. Além do conteúdo de fácil acesso, que contabiliza aproximadamente 4% de toda a informação em rede, existe também o conteúdo de difícil acesso, contabilizando os 96% restantes. Essa informação de difícil acesso se encontra na *Deep Web*, que é uma camada mais profunda da internet, onde estão informações sigilosas e conteúdos ilegais, que não poderiam ser colocados na web convencional[26], e para acessar tal rede é necessário fazer alguns procedimentos. Normalmente esses conteúdos são colocados lá por conta do difícil acesso e pela maior facilidade de se esconder. Dentro desses conteúdos pode ser encontrado material ensinando como criar por exemplo um *malware* como o *ransomware.* Também é comum nos links a presença do próprio *ransomware* nessa rede, infectando assim os usuários convencionais.

Adiante entraremos na seara do funcionamento do *ransomware*, assim como cada passo para sua manifestação total, à luz do direito.

---

25. POLICARPO, Poliana; BENNARD, Edna. *Cibercrimes na E-Democracia*. Op. cit., p. 169.
26. POLICARPO, Poliana; BENNARD, Edna. *Cibercrimes na E-Democracia*. Op. cit., p. 202.

7.3 Passos do *Ransomware* à Luz do Direito

Elencar as violações causadas por um ciberataque causado por um *ransomware* é uma tarefa difícil. Várias garantias constitucionais, tanto brasileiras quanto portuguesas, são feridas, como também vários tratados de direitos humanos. Delimitaremos tal pesquisa à luz do direito penal brasileiro e da convenção de Budapeste, muito embora em alguns momentos serão utilizados outros códigos, na tentativa de promover um melhor entendimento.

O que é a Convenção de Budapeste? Esta convenção recebeu esse nome por ter sido adotada em Budapeste, muito embora seja a Convenção do Conselho da Europa sobre o Cibercri-me. Mesmo estando dentro do quadro do Conselho Europeu, é uma convenção internacional[27]. Vários outros países não mem-bros do conselho da Europa também são signatários, como os Estados Unidos, Japão, Canadá, África do Sul, Israel, Chile, entre outros; tendo a convenção entrado em vigor no dia 1º de julho de 2004.[28]

Muitos países se tornaram signatários desde o decorrer de sua existência, a Lei 109, de 2009 de Portugal, "estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico, transpondo para a ordem jurídica inter-na a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa".

Já no Brasil, através do Decreto 11.491 de 2023, "fica promulgada a Convenção sobre o Crime Cibernético, firmada em

27. MASSENO, Manuel David; WENDT, Emerson. "O ransonware na Lei: apontamentos breves do direito português e brasileiro". Disponível em: http://direitoeti.com.br/artigos/o-ransomware-na-lei-apontamentos-breves-de-direito-portugues-e-brasileiro/. Acesso em: 6 dez. 2017.

28. COUNCIL OF EUROPE. "Convention on Cybercrime". Disponível em: http://www.migliorisiabogados.com/wp-content/uploads/2014/04/Convencion-de-Budapest-firmantes-Convecion-contra-el-cibercrimen.docx. Acesso em: 15 dez. 2017.

Budapeste, em 23 de novembro de 2001", ainda assim será comparado com os tipos penais presentes.

Ao dar andamento, vivemos em uma era na qual a informação se tornou o petróleo do mundo. É a base para a mineração de dados, para o desenvolvimento de inteligências artificiais, assim como um objeto de negociação valioso.

O que têm a ver informação e *big data*? Tudo! *Big data* significa uma grande quantidade de dados. Assim, estamos presenciando uma época em que há uma acumulação excessiva de dados, seja nos computadores, seja nos *smartphones*, seja nos meios de armazenamento na nuvem, como fotos, músicas, vídeos e documentos digitais[29]. E quando esses dados são coletados por um terceiro não autorizado, sem que o usuário perceba, e expostos na internet, causam violação da honra, assim como violação da privacidade e da intimidade de tal usuário, ferindo assim a sua dignidade. O fato citado neste parágrafo é mais comum do que se imagina.

Diante da disponibilidade das informações, o *ransomware* ataca, privando o proprietário de acessá-las. Segundo Poliana Policarpo e Edna Bennard, existem algumas etapas da propagação de uma ameaça avançada pela internet[30]. Unindo essas etapas com a abordagem que o Manuel David Masseno e o Emerson Wendt[31] fizeram sobre o *ransomware*, a seguir veremos uma sequência de atos ilícitos causados pelo *ransomware*, olhando pela ótica da propagação por meio do correio eletrônico.

7.3.1 Planejamento

Esta é a fase do reconhecimento, em que o criminoso irá identificar vítimas em potencial, analisando as suas informações e seu histórico de pesquisa para criar iscas específicas,

29. DAVENPORT, Thomas H. *Big Data no Trabalho: Derrubando mitos e descobrindo oportunidades*. Trad.: de Cristina Yamagami. Rio de Janeiro: Elsevier, 2014. Op. cit., p. 17.
30. POLICARPO, Poliana; BENNARD, Edna. *Cibercrimes na E-Democracia*. Op. cit., p. 296.
31. MASSENO, Manuel David; WENDT, Emerson. *O ransonware na Lei*. Ibidem.

como, por exemplo, bancos, hospitais, órgãos do governo. Muito embora este tópico vise direcionar tal estudo para o direito penal brasileiro e a convenção de Budapeste, esta etapa do planejamento será apresentada à luz das leis de combate ao terrorismo brasileiro e português.

A legislação de combate ao terrorismo portuguesa[32], em seu art. 5-A, 1:

> Quem, por quaisquer meios, direta ou indiretamente, fornecer, recolher ou detiver fundos ou bens de qualquer tipo, bem como produtos ou direitos suscetíveis de ser transformados em fundos, com a intenção de serem utilizados ou sabendo que podem ser utilizados, total ou parcialmente, no **planeamento**, na preparação ou para a prática dos factos previstos no n.º 1 do artigo 2.º, quer com a intenção nele referida quer com a intenção referida no n.º 1 do artigo 3.º, é punido com pena de prisão de 8 a 15 anos.

A lei brasileira 13.260[33], de 16 de março de 2016, diz em seu art. 5º:

> Realizar atos **preparatórios** de terrorismo com o propósito inequívoco de consumar tal delito.

Assim, diante das legislações que combatem o terrorismo, tanto a portuguesa quanto a brasileira, vemos que há uma previsão de o planejamento como ato terrorista, assim, o próprio desenvolvimento do código malicioso quando da elaboração do e-mail falso já configuraria o crime.

7.3.2 Enganar o usuário

Após o conteúdo do e-mail ter sido criado ainda na fase de planejamento, ele será enviado para várias pessoas, que também já tinham o endereço eletrônico pesquisado.

32. Lei 52/2003, de 22 de agosto. *Lei de Combate ao Terrorismo*. Ibidem.
33. Lei 13.260/2016, de 16 de março. 2016. *Lei Antiterrorismo*. Ibidem.

A Convenção de Budapeste diz, no art. 7º[34]:

> Artigo 7º – **Falsidade informática** [...] [...] a introdução, a alteração, a eliminação ou a supressão intencional e ilegítima de dados informáticos, produzindo dados não autênticos, com a intenção de que estes sejam considerados ou utilizados para fins legais como se fossem autênticos, quer sejam ou não directamente legíveis e inteligíveis. Uma Parte pode exigir no direito interno uma intenção fraudulenta ou uma intenção ilegítima similar para que seja determinada a responsabilidade criminal. (grifo nosso)

Diz o Código Penal Brasileiro, nos arts. 171 e 299[35]:

> **Estelionato –** Art. 171. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
>
> **Falsidade ideológica** – Art. 299. Omitir, em documento público ou particular, declaração que dele devia constar, ou nele inserir ou fazer inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar, obrigação ou alterar a verdade sobre fato juridicamente relevante:

Neste contexto, tratamos do envio de um e-mail com código malicioso que aparenta vir de fontes seguras, enganando, assim, os usuários, fazendo com que caiam nas iscas e logo depois são redirecionados para sites que possuem aspecto seguro e confiável, porém possuem caráter malicioso, ou simplesmente no próprio e-mail, ao abrir um arquivo em anexo, inicia-se a invasão.

34. Convenção de Budapeste. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso: 6 dez. 2017.

35. Decreto-Lei 2848/1940, de 07 de dezembro. "Código Penal Brasileiro". Disponível em: http://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-2848-7-dezembro-1940-412868-normaatualizada-pe.doc. Acesso em: 6 dez. 2017.

7.3.3 Violar a segurança do sistema informático

Após a invasão, já estará sendo aberta uma vulnerabilidade no sistema do usuário, permitindo que o *hacker* tenha acesso diretamente ao conteúdo no dispositivo informático ou permitindo que o *ransomware* se propague automaticamente, iniciando seu processo de encriptação das informações.

A Convenção de Budapeste, nos arts. 2º e 3º[36], diz:

> Artigo 2º – **Acesso ilegítimo** [...] [...] o acesso intencional e ilegítimo à totalidade ou a parte de um sistema informático. As Partes podem exigir que a infracção seja cometida com a violação de medidas de segurança, com a intenção de obter dados informáticos ou outra intenção ilegítima, ou que seja relacionada com um sistema informático conectado a outro sistema informático. (grifo nosso)
>
> Artigo 3º – **Intercepção ilegítima** [...] [...] a intercepção intencional e ilegítima de dados informáticos, efectuada por meios técnicos, em transmissões não públicas, para, de ou dentro de um sistema informático, incluindo emissões electromagnéticas provenientes de um sistema informático que veicule esses dados. As Partes podem exigir que a infracção seja cometida com dolo ou que seja relacionada com um sistema informático conectado com outro sistema informático. (grifo nosso)

Diz o Código Penal Brasileiro, no art. 154-A[37]:

> **Invasão de Dispositivo Informático**. Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita. (grifo nosso)

A inserção do código malicioso, ou *malware*, pode ocorrer por duas principais motivações; o ciberterrorismo, que é o caso supracitado, que não visa apenas um indivíduo em particular e sim causar terror de forma mais generalizada, ou pode também

36. Convenção de Budapeste. Ibidem.
37. Decreto-Lei 2848/1940, de 07 de dezembro. Ibidem.

ser voltada para prejudicar um indivíduo em particular. Essa inserção tendo a finalidade de causar terror pelo terrorismo cibernético é tipificada como ação penal pública, porém, quando visa prejudicar o indivíduo de forma particular, por via de um ataque direcionado, é tipificada como inserção de código malicioso[38].

7.3.4 Encriptação dos dados

Conforme apresentado anteriormente, a encriptação é o meio mais seguro para se proporcionar a confidencialidade, mas, quando é utilizada por um *hacker* para sequestrar informações, ele exigirá o pagamento de um resgate para decriptar (ou não, visto que o pagamento do resgate não garante que as informações estarão disponíveis novamente).

A disponibilidade é um dos princípios da segurança da informação e significa que toda e qualquer informação deve estar disponível sempre que necessária e torná-la indisponível fere tal princípio, assim como quebra as políticas de segurança determinadas pelo trabalho de *compliance* digital.

A Convenção de Budapeste diz, nos arts. 4º, 5º e 8º[39]:

> Artigo 4º – **Interferência em dados** – 1. [...] [...] o acto de intencional e ilegitimamente danificar, apagar, deteriorar, alterar ou eliminar dados informáticos. 2. Uma Parte pode reservar-se o direito de exigir que a conduta descrita no n.º 1 provoque danos graves. (grifo nosso)
>
> Artigo 5º – **Interferência em sistemas** [...] [...] a obstrução grave, intencional e ilegítima, ao funcionamento de um sistema informático, através da introdução, transmissão, danificação, eliminação, deterioração, modificação ou supressão de dados informáticos. (grifo nosso)
>
> Artigo 8º – **Burla informática** [...] [...] o acto intencional e ilegítimo, que origine a perda de bens a terceiros através: a) Da introdução, da alteração, da eliminação ou da supressão de dados informáticos, b) de qualquer intervenção no funcio-

38. SYDOW, Spencer Toth. *Crimes informáticos e suas vítimas*. São Paulo: Saraiva, 2013. p. 129.

39. *Convenção de Budapeste.* Ibidem.

> namento de um sistema informático, com a intenção de obter um benefício económico ilegítimo para si ou para terceiros. (grifo nosso)

Já o Código Penal Brasileiro diz, nos arts. 154-A[40], 265 e 266[41]:

> **Invasão de Dispositivo Informático**. Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de **obter, adulterar ou destruir dados ou informações** sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita. (grifo nosso)
>
> **Atentado contra a segurança de serviço de utilidade pública –** Art. 265. Atentar contra a segurança ou o funcionamento de serviço de água, luz, força ou calor, ou qualquer outro de utilidade pública: (grifo nosso)
>
> **Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública –** Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: (grifo nosso)

Diante do exposto nos artigos da convenção de Budapeste, a interferência de dados, interferência de sistemas e a burla informática estão ligados diretamente por indisponibilizarem o que está contido no dispositivo informático invadido pelo *ransomware*.

Já no Código Penal Brasileiro foram incluídos os artigos 265 e 266, visto que o direito à informação é um direito fundamen-tal garantido tanto pela Constituição Federal Brasileira quanto pela Constituição da República Portuguesa, assim, o interrompimento da informação de várias pessoas por um ato ciberterrorista estará violando garantias constitucionais. Para tanto, também foi criado o art. 154-A da Lei Carolina Dieckmann, trata não só da violação da segurança, mas também da obtenção, alteração e/ou destruição dos dados e ou informações em dispositivos informáticos, posteriormente alterado pela Lei 14.155, que também aborda sobre estelionato e furto eletrônicos.

40. Decreto-Lei 2848/1940, de 07 de dezembro. Ibidem.
41. Decreto-Lei 2848/1940, de 07 de dezembro. Ibidem.

Caso for realizado ou facilitado por funcionado público, a depender do caso, poderá se encaixar nos tipos penais que es-tão ligados à corrupção digital. Seria o caso de ser um cibercriminoso ou ciberespião infiltrados no sistema público.

No caso do cibercriminoso:

> Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de da-dos da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano.
>
> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:

No caso de uma espécie de ciberespião, mas com a intenção de sabotagem, incluído pelo tipo ascendido pela lei que trata sobre o Estado Democrático de Direito, Lei 14.197, no que toca o artigo que aborda sobre a sabotagem.

> Art. 359-R. Destruir ou inutilizar meios de comunicação ao público, estabelecimentos, instalações ou serviços destina-dos à defesa nacional, com o fim de abolir o Estado Democrá-tico de Direito.

Nesse caso, poderia ser realizado por qualquer um, mas com a intenção de abolir o Estado Democrático de Direito.

7.3.5 Pagamento (ou não) para o resgate das informações

O *ransomware* é um vírus sequestrador que codifica as informações do computador da vítima através da encriptação dos arquivos e cobra um valor pelo resgate. Esse valor geralmente é exigido para ser pago usando uma criptomoeda, e a mais comum é a *bitcoin,* que é uma moeda digital. O pagamento feito por meio dessa moeda torna praticamente impossível o rastreio para se chegar ao criminoso[42].

42. TECHTUDO. "O que é o ransomware?". Disponível em: http://www.techtudo.com.br/noticias/noticia/2016/06/o-que-e-ransomware.html. Acesso em: 6 dez. 2017.

Diz a Convenção de Budapeste, no art. 8º, *b*[43]:

> Artigo 8º – **Burla informática** [...] [...] o acto intencional e ilegítimo, que origine a perda de bens a terceiros através: b) de qualquer intervenção no funcionamento de um sistema informático, com a intenção de obter um **benefício económico** ilegítimo para si ou para terceiros. (grifo nosso)

Já o Código Penal Brasileiro diz, no art. 158[44]:

> **Extorsão**: Art. 158. Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem **indevida vantagem econômica**, a fazer, tolerar que se faça ou deixar de fazer alguma coisa. (grifo nosso)

Tanto na Convenção de Budapeste quanto no Código Penal Brasileiro fica prevista a indevida vantagem econômica paga em troca de que as informações sejam decrepitadas. Mas tudo pode ocorrer diferentemente, no caso de o cibercriminoso não decrepitar as informações memo após o pagamento do resgate.

Diz o Código Penal Brasileiro, no art. 171[45]:

> **Estelionato**: Art. 171. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:

No caso da não liberação dos arquivos, em Portugal novamente caberia o já citado anteriormente crime de burla, previsto pelo art. 8, *b* da Convenção de Budapeste, muito embora no Brasil já teria a tipificação penal supracitada, como também caberia o também citado anteriormente art. 154-A.

7.3.6 Liberação dos dados

A liberação dos dados sequestrados é para ocorrer logo após o pagamento e inserção da chave liberada pelo *hacker*,

43. Convenção de Budapeste. Ibidem.
44. Decreto-Lei 2848/1940, de 07 de dezembro. Ibidem.
45. Idem, Ibidem.