ISSN 2447-1097

Direito & TI – Porto Alegre / RS www.direitoeti.com.br

O *RANSOMWARE* NA LEI: APONTAMENTOS BREVES DE DIREITO PORTUGUÊS E BRASILEIRO[i]

Manuel David Masseno[1]

Emerson Wendt[2]

[1] Em matéria de Direito & TI, é Professor Adjunto do Instituto Politécnico de Beja, em Portugal, onde é também Pesquisador Sénior no Laboratório UbiNET – Segurança Informática e Cibercrime e Membro da Coordenação do MESI – Mestrado em Engenharia de Segurança Informática, além de ter vindo a lecionar, como convidado, na Escola de Direito da Universidade do Minho, na Faculdade de Direito da Universidade de Lisboa, no Centro de Estudos Sociais e no Centro de Estudos Notariais e Registais da Universidade de Coimbra, na Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa e no Centro de Estudos Judiciários, integrando ainda os Órgãos Sociais da ISOC-Portugal – *Internet Society-Portugal Chapter*, o Fórum Jurídico e o Grupo Permanente de Segurança e Privacidade da Associação para a Promoção e Desenvolvimento da Sociedade da Informação, além de pertencer à Comissão Científica da revista *Cyberlaw by CIJIC*, do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa. No Brasil, lecionou, como Professor Visitante, nas Universidades Federais de Santa Catarina, de Santa Maria (RS) e do Paraná, na Faculdade Damásio de Jesus (SP) e na Escola Paulista da Magistratura, é também Diretor para as Relações Internacionais do IBDI – Instituto Brasileiro de Direito da Informática e Membro Consultor da Comissão de Direito Digital e *Compliance* da Ordem dos Advogados do Brasil / Seção de São Paulo, assim como das Comissões de Direito Digital da Subseção de Campinas e de Informática Jurídica e Direito Eletrônico da de Santos, além de pertencer ao Grupo de Estudos Temático em Direito Digital e *Compliance* da FIESP - Federação das Indústrias do Estado de São Paulo e ser Pesquisador do GEDEL - Grupo de Pesquisa "Justiça e Direito Eletrônicos" da Escola Judicial do Tribunal Regional do Trabalho - 3ª Região (MG), e integrar o Conselho Editorial e Científico Nacional e Internacional da REDESG – *Revista Direitos Emergentes na Sociedade Global*, da Universidade Federal de Santa Maria (RS). Em termos internacionais, integra a Rede Temática Europeia LEFIS - *LEgal Framework for the Information Society*, a Rede CIIDI – Rede Ibero-Americana de Universidades e Institutos com Investigação em Direito e Informática, bem como ao Consórcio Internacional sobre Tecnologias Convergentes *LexConverge*, além estar na EPE – *Europol Platform for Experts*, em especial na EDEN – *Europol Data Protection Experts Network* e na EC3 SPACE – *Secure Platform for Accredited Cybercrime Experts*, integrando ainda os Conselhos Editoriais da *International Review of Law, Computers & Technology* e do *European Journal of Law and Technology*, ambas publicadas no Reino Unido, da *Medialaws - Law and Policy of the Media*, na Itália, e da *Безпека інформації* / *Information Security*, na Ucrânia. E-mail: mdmasseno@gmail.com.

[2] Delegado de Polícia Civil do RS. Chefe da Polícia Civil no RS e Presidente do Conselho Superior de Polícia da Polícia Civil do RS. Formado em Direito pela Faculdade de Direito da Universidade Federal de Santa Maria e Pós-graduado em Direito pela URI-Frederico Westphalen. Mestre em Direito pelo UnilaSalle Canoas-RS. Ex-Diretor do Departamento Estadual de Investigações do Narcotráfico e Ex-Diretor do Gabinete de Inteligência e Assuntos Estratégicos. Professor da Academia de Polícia Civil nas cadeiras de Inteligência Policial e Investigação Criminal. Também, é professor dos cursos de pós-graduação e/ou extensão da UNISINOS (São Leopoldo-RS), SENAC-RS (Passo Fundo-RS), IDC (Porto Alegre-RS), Verbo Jurídico (Porto Alegre-RS), Uniritter (Porto Alegre-RS e Canoas-RS), EPD (São Paulo-SP), IMED (Passo Fundo-RS e Porto Alegre-RS), UNITOLEDO (Porto Alegre-RS), ESMAFE/RS (Porto Alegre), Uninorte (Rio Branco-AC), Unifacs (Salvador-BA). Membro da Associação Internacional de Investigação de Crimes de Alta Tecnologia (HTCIA), do PoaSec e do INASIS, além de ex-integrante do Comitê Gestor de Tecnologia da Informação da Secretaria de Segurança Pública do RS. Já ministrou aula nas Academias das Polícia Civis de Pernambuco, Goiás, Paraná, Acre, Alagoas, Sergipe, Rondônia e Piauí. Também, é Tutor dos cursos EAD e presenciais da Secretaria Nacional de Segurança Pública, especialmente na atividade de Inteligência de Segurança Pública. Autor do livro Inteligência Cibernética (Editora Delfos) e coautor dos livros "Crimes Cibernéticos: ameaças e procedimentos de investigação", com Higor Vinícius Nogueira Jorge, "Inteligência Digital", com Alesandro Gonçalves Barreto, "Investigação Digital em Fontes Abertas", com Alessandro Gonçalves Barreto e Guilherme Caselli (Ed. Brasport). Autor e organizador dos livros "Investigação Criminal: ensaios sobre a arte de investigar crimes" (Ed. Brasport) e "Investigação Criminal: Provas" (Ed. Livraria do Advogado), juntamente com o Fábio Motta Lopes.

ISSN 2447-1097

Direito & TI – Porto Alegre / RS www.direitoeti.com.br

RESUMO

Este artigo visa enquadrar juridicamente o chamado *ransomware* frente às previsões normativo-penais nas legislações portuguesa e brasileira, sendo aquela em particular determinada pelas fontes internacionais e europeia. O objetivo é conduzir a um melhor entendimento das atuais respostas de natureza penal a tais ataques. Atendendo aos objetivos deste trabalho, a fundamentação teórica foi deixada implícita, inclusive para facilitar a respetiva compreensão, inclusive para quem não tem formação jurídica.

Palavras-chave: Portugal; Brasil; direito penal; Europa; *ransomware*.

INTRODUÇÃO

A disseminação de ataques informáticos utilizando *ransomware* chamou a atenção mundial no primeiro semestre de 2017. Foram colocados em cheque sistemas tecnológicos e jurídicos, exigindo análises quanto ao contingenciamento quando de sua ocorrência. Tais ataques, que vinham sendo isolados, acabaram por proliferar após o *WannaCry*[ii], um ataque de *ransomware* em larga escala e com múltiplas vítimas, também em Portugal e no Brasil.

Deste modo, é fundamental que a presente análise se inicie pela caraterização do protocolo que constitui o *modus operandi* no *ransomware*[iii]. Por outras palavras, sem o preenchimento de cada um deles e por esta sequência, até poderemos ter ataques maliciosos mas não se tratará de ataques de *ransomware*. Ter sido esse o caso do (*Not*)*Petya*[iv], no qual a finalidade última foi a obtenção de informações confidenciais, além de tornar inoperantes os sistemas atacados. Em extrema síntese, o mesmo pode-se resumir em quatro passos, todos eles necessários para a identificação do nosso objeto:

(**1**) a obtenção de acesso ao sistema informático da vítima, com ou sem engano, por parte do(s) autore(s);

(**2**) a que se segue a inserção no referido sistema de um código, o qual encripta dados, com base em um mecanismo de chaves assimétricas, gerando adicionalmente uma identificação personalizada desse mesmo sistema;

(**3**) depois, tem lugar uma comunicação à vítima do ocorrido, assim como do montante exigido, para facultar/entregar a chave personalizada de desencriptação, enviando valores em criptomoedas (para não ser rastreável), e o endereço (carteira) para onde deve ser enviado, junto com a identificação personalizada do sistema em causa; e

(**4**) finalmente, uma vez, efetuado o pagamento, a vítima recebe uma chave personalizada de desencriptação que lhe permite recuperar os dados.

Com essa técnica, apesar de os pedidos de resgate não costumarem ultrapassar os 500 Dólares,

Autor do Livro “Internet & Direito Penal: Risco e Cultura do Medo” (Ed. Livraria do Advogado). E-mail: emersonwendt@gmail.com.

os criminosos digitais tendem a obter um valor global elevado[v]. Além disso, podem continuar com tais práticas devido à passividade das vítimas, até por ser frequente que os administradores dos sistemas ou as diretorias das organizações paguem os resgates, evitando os "custos reputacionais" que lhes adviriam se a ocorrência de tais ataques viesse a ser conhecida, não reportando, internamente, e/ou apresentando queixa junto das Polícias ou do Ministério Público.

Também, é evidente que se trata de ataques de escala internacional, quase sempre provenientes do Exterior, com as inerentes dificuldades técnicas de rastreamento. Dificuldades essas a que se juntam as jurídicas, sobretudo quando a cooperação policial internacional é dificultada pela não pertença a redes internacionais, como ocorre com o Brasil relativamente à instituída pela *Convenção de Budapeste*. No entanto, não é este o objetivo deste breve estudo, o qual se restringe pelo Direito Penal Material.

Desde estas bases, revisar-se-á as possibilidades de qualificação (jurídico-penal) dos ataques de *ransomware*, desde as fontes legislativas portuguesa e brasileira.

1. A AUSÊNCIA DE UMA TIPIFICAÇÃO ESPECÍFICA

Tratando-se de uma técnica disseminada mundialmente há pouco tempo, o *ransomware*, nos precisos termos antes descritos, não está tipificado *qua tale* e a necessidade de uma tal tipificação é objeto de debate no âmbito da Política Legislativa, pois as respostas que constam das atuais fontes podem ser bastantes para o combater com a devida eficácia.

A exceção está nos Estados Unidos, apesar de o *ransomware* apenas ser referido no Wyoming (WY Stat § 6-3-506, 2016) e tipificado na Califórnia (Section 523 (c) do *Penal Code*, em vigor desde 1 de janeiro de 2017), decorrendo um processo legislativo orientado no mesmo sentido no Maryland. Como podemos constatar, a previsão do *Penal Code* californiano corresponde à caraterização enunciada:

> *'Ransomware' means a computer contaminant, as defined in Section 502, or lock placed or introduced without authorization into a computer, computer system, or computer network that restricts access by an authorized person to the computer, computer system, computer network, or any data therein under circumstances in which the person responsible for the placement or introduction of the ransomware demands payment of money or other consideration to remove the computer contaminant, restore access to the computer, computer system, computer network, or data, or otherwise remediate the impact of the computer contaminant or lock* (*Section* 523 (c) (1)

Por isso, é mesmo necessário compulsar as fontes potencialmente aplicáveis a esta realidade, de modo a construir respostas integradas e eficazes.

Assim, no que se refere a Portugal, temos à disposição o *Código Penal* (de 1995, com múltiplas atualizações), a *Lei do Cibercrime* (Lei n.º 109/2009, de 15 de setembro) e, também, a *Lei da Proteção de Dados Pessoais* (Lei n.º 67/98, de 26 de outubro). A este propósito, é necessário ter em atenção que, desde a *Lei da Criminalidade Informática* (Lei n.º 109/91, de 17 de agosto), o conteúdo do Direito português resulta essencialmente da aplicação ou transposição de Instrumentos Normativos de origem europeia, os quais relevam também para a interpretação das Leis nacionais. Nomeadamente, nos importam a *Convenção do Conselho da Europa sobre o Cibercrime*, adotada em Budapeste, a 23 de novembro de 2001, e a Diretiva 2013/40/UE, do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa aos ataques contra os sistemas de informação.

Por seu turno, no Brasil as fontes têm evoluído mais lentamente e com uma influência externa apenas indireta, pelo que podemos encontrar apoios no *Código Penal* (de 1942), tal como alterado pela *Lei Carolina Dieckmann* (Lei 12.737/2012, de 30 de novembro). O Brasil não é signatário da *Convenção do Conselho da Europa sobre o Cibercrime*, denominada de *Convenção de Budapeste*, apesar de a mesma estar aberta à adesão de outros países e de, na América Latina, tal já ser o caso do Chile, do Panamá e da República Dominicana, enquanto os Estados Unidos, o Canadá, o Japão e a República da África do Sul participaram mesmo na negociação da *Convenção*.

2. A OBTENÇÃO DE ACESSO AO SISTEMA

Antes de mais, é preciso ter em mente que a obtenção de acesso ao sistema informático, o primeiro passo do protocolo de um ataque de *ransomware*, pode ocorrer *com* e *sem engano* do respetivo titular.

Embora seja mais frequente que o acesso ao sistema seja obtido através de práticas maliciosas, começaremos por enfrentar a possibilidade de o mesmo ocorrer por meios técnicos, dispensando a indução em erro do seu titular.

Assim, no que se refere há legislação portuguesa, está tipificado o crime de **acesso ilegítimo** (Art.º 6.º da *Lei do Cibercrime*, o qual segue o disposto no Art.º 2.º da *Convenção de Budapeste* e Art.º 3.º da Diretiva europeia relativa aos ataques a sistemas informáticos, embora com uma menor tolerância do que a permitida por estas Fontes relativamente ao chamado "*hacking* de chapeu branco"):

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

A mesma pena é aplicável também:

> 2. [a] quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as ações não autorizadas descritas no número anterior. (Na sequência do disposto no Art.º 6.º da *Convenção de Budapeste* e do Art.º 7.º da Diretiva relativa aos ataques contra sistemas de informação)

Nestas previsões normativas, o bem jurídico penalmente protegido é a segurança na aceção de disponibilidade exclusiva do sistema informático pelo seu titular.

Porém, em grande parte dos casos será preenchido um tipo diferente, o correspondente ao crime de *acesso indevido* (Art.º 44.º da *Lei da Proteção de Dados Pessoais*), cujos bens jurídicos penalmente protegidos são, antes, a privacidade e a autodeterminação informacional:

> 1. Quem, sem a devida autorização, por qualquer modo, aceder a dados pessoais cujo acesso lhe está vedado é punido com prisão até um ano ou multa até 120 dias.

A maior frequência do preenchimento da previsão do crime de **acesso indevido**, comparativamente com o de **acesso ilegítimo**, decorre da circunstância de a generalidade dos sistemas informáticos conterem dados pessoais, em sentido técnico, isto é:

> […] qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular [física, na terminologia brasileira] identificada ou identificável («titular dos dados»); é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social; (Art.º 3.º alínea a) da mesma *Lei*)

Mais ainda, a respetiva aplicabilidade foi ampliada pelo disposto no *Novo Regulamento Geral sobre a Proteção de Dados da União Europeia* (Art.º 4.º 1. do Regulamento 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016), em cujos termos são "dados pessoais":

> [toda] informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular [física, na terminologia brasileira].

No entanto, o mais comum é o *ransomware* ser introduzido no sistema enganando o seu titular, através do chamado *Phishing*. Nomeadamente, através de uma mensagem falsa de correio

eletrônico, ou de um aplicativo de comunicação, através da qual o autor cria a aparência de se tratar de um remetente de confiança da vítima, ou de um seu colaborador, a induzindo a pressionar um anexo ou a seguir um *link*.[vi]

Na legislação portuguesa e antes de mais, uma tal prática poderá corresponder ao crime de **falsidade informática** (Art.º 3.º da *Lei do Cibercrime*, em consonância com o Art.º 7.º da *Convenção de Budapeste*):

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

Aqui, o bem jurídico protegido é o interesse público na preservação da confiança no tráfego jurídico. O que conduz a Jurisprudência portuguesa, embora com algumas reservas da Doutrina, a entender que, no *Phinshing*, existe um concurso real com um outro tipo, o do crime de **burla informática** *e nas comunicações* (Art.º 221.º do *Código Penal*, além do Art.º 7.º da *Convenção de Budapeste*). Neste e diferentemente, o bem protegido é já o patrimônio da vítima, o sendo apenas a tutela da confiança no tráfego jurídico em termos reflexo. Deste modo, é punido:

> 1. Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorreta de programa informático, utilização incorreta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento […]

Pela legislação brasileira, temos a chamada *Lei Carolina Dieckmann* (Lei 12.737/2012, de 30 de novembro), que acresceu no *Código Penal Brasileiro* o Art.º 154-A, criminalizado a **invasão de dispositivo informático**, a qual consiste na ação de:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1.º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> […]
> § 3.º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

Consequentemente, a invasão apenas é penalizada se ocorrer "mediante violação indevida de mecanismo de segurança" e "sem autorização expressa ou tácita do titular do dispositivo" (*Caput* do Art.º), isto é, se ocorrer por meios técnicos que dispensem a intervenção deste, não relevando a respetiva vontade, viciada ou não por erro.

Por outro lado e tal como na portuguesa, para a lei brasileira não só quem dissemina o código malicioso comete o crime, mas também quem o produz, modifica ou vende (§ 1.º). É ainda de sublinhar que há aumento de pena (majorante), e um crime mais grave, se existir "um controle remoto não autorizado do dispositivo invadido." (§ 3.º *in fine*)

Mas, como vimos, o *Phishing* é uma via bastante mais comum de disseminação de códigos maliciosos. Ora, atendendo à respetiva caraterização, poderemos ter um crime de **falsidade ideológica** (Art.º 299.º do *Código Penal*), consistente em:

> 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:
> Pena - reclusão, de um a cinco anos, e multa, se o documento é público, e reclusão de um a três anos, e multa, se o documento é particular.

Em concurso material, com o de **estelionato** (Art.º 171.º do *Código Penal*), inclusive por os bens jurídicos penalmente protegidos serem análogos aos da legislação portuguesa, o qual é praticado através da ação de:

> 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:
> Pena - reclusão, de um a cinco anos, e multa.

Há que se ponderar que, dentre os dois últimos delitos citados, é muito mais comum e factível a ponderação e capitulação em relação ao delito de estelionato. Porém, é necessário ter em conta que, em nenhum dos casos, há previsão normativa especificamente orientada e dirigida para os aspectos tecnológico-digitais, diferentemente do que ocorre na legislação portuguesa.

3. O TORNAR OS DADOS INACESSÍVEIS

Um passo essencial à caraterização tipológica do *ransomware* é o da encriptação/encriptamento do sistema informático atacado, no todo ou em parte, ficando os dados indisponíveis para o respetivo titular.

Na legislação portuguesa, uma tal ação preenche os pressupostos do crime de **sabotagem informática** (Art.º 5.º da *Lei do Cibercrime*, no seguimento da previsão do Art.º 5.º da *Convenção de Budapeste* e em consonância com o Art.º 4.º da Diretiva europeia relativa aos ataques a sistemas informáticos). Por este, são protegidos não só bens privados como o património e a disponibilidade do sistema informático pelo respetivo titular, mas também bens públicos como a continuidade da vida em sociedade. Pelo que se trata de:

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

Este enquadramento é igualmente aplicável a

> 2. […] quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as ações não autorizadas descritas no número anterior. (Em linha com o disposto no Art.º 6.º *da Convenção de Budapeste* e no Art.º 7.º da Diretiva europeia relativa aos ataques contra sistemas informáticos)

Além disso, existem formas qualificadas deste crime, às quais corresponderá uma pena "de prisão de 1 a 10 anos.", quando e se "O dano emergente da perturbação for de valor consideravelmente elevado […] ou "A perturbação causada atingir de forma grave ou duradoura um sistema informático que apoie uma atividade destinada a assegurar funções sociais críticas, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos. (n.º 5 a) e b), também com arrimo ao previsto no Art.º 9.º n.º 4 da Diretiva europeia relativa aos ataques),

Isto é, quando são atingidas "infraestruturas críticas", entendidas como:

> […] a componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas

> funções. (Art.º 2.º a) do Decreto-Lei n.º 62/2011, de 9 de maio, resultante da transposição do, também, Art.º 2.º a) da Diretiva 2008/114/CE, do Parlamento Europeu e do Conselho, de 8 de dezembro)

Às quais temos de acrescentar os sistemas informáticos que pertençam aos operadores "de serviços essenciais" (Art.º 4.º 4) da Diretiva 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, ainda não transposta para o Ordenamento português).

Quanto à legislação brasileira, na falta de um tipo análogo ao da *sabotagem informática*, a identificação da relevância penal da encriptação/encriptamento inerente ao *ransomware* é mais difícil, inclusive por não se estar perante uma destruição dos danos, mas apenas de uma indisponibilização temporária do sistema informático para a vítima, conforme ao plano criminoso subjacente ao protocolo enunciado.

Por isso mesmo, temos de distinguir as situações nas quais os bens jurídicos penalmente protegidos são de natureza privada, como património e a disponibilidade do sistema informático pelo respetivo titular, daquelas em que estão em causa bens públicos, incluindo até a continuidade da vida em sociedade.

No que se refere às primeiras, podemos encontrar um ponto de apoio no disposto pela *Lei Carolina Dieckmann*, sempre que o acesso haja resultado de uma invasão de dispositivo informático, nos termos acima enunciados, ou seja:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita (*Caput* do Art.º 154-A do *Código Penal*)

Inclusive porque, entre as variantes do dolo específico requerido, isto é, "adulterar ou destruir dados ou informações", pode caber o encriptamento/encriptação sem ser tangido o Princípio da Tipicidade Penal, constitucionalmente garantido (Art.º 5.º inciso XXXIX da *Constituição Federal*).

No que se refere às situações em que ficam em causa bens públicos essenciais, temos o crime de **atentado contra a segurança de utilidade pública** (Art.º. 265.º do *Código Penal*), o qual passa por:

> Atentar contra a segurança ou o funcionamento de serviço de água, luz, força ou calor, ou qualquer outro de utilidade pública:
> Pena - reclusão, de um a cinco anos, e multa.

[…].

E, mais ainda, o de **interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade** (Art.º 266.º do mesmo *Código*), que se traduz em:

> Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
> Pena - detenção, de um a três anos, e multa.
> § 1.º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
> § 2.º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.

Sendo de ter em especial atenção o § 1.º do Art.º 266.º, por fazer referência expressa à interrupção de serviço telemático ou de informação de utilidade pública, impedindo ou dificultando-lhe o restabelecimento, o que ocorre com o protocolo *ransomware*, especialmente em casos como o do *Petya*.

4. COM PEDIDO DE RESGATE

Tanto a legislação portuguesa quanto a brasileira são claras ao caraterizar o protocolo inerente ao *modus operandi* do *ransomware* como correspondendo ao crime de **extorsão**. Aliás, a referida *Section* 523 do *Penal Code* do Estado da Califórnia prevê uma forma qualificada de *extorsão*, a qual é definida como "*Extortion is the obtaining of property from another, with his consent, or the obtaining of an official act of a public officer, induced by a wrongful use of force or fear, or under color of official right*.". (*Section* 518). Ademais, em ambos Ordenamentos, o bem jurídico penalmente protegido é a liberdade de disposição do seu patrimônio pela vítima.

Assim, na legislação portuguesa, se trata de punir a conduta de (Art.º 223.º do *Código Penal*):

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

Este crime pode assumir uma forma qualificada, passando a caber uma "pena de prisão de 3 a 15 anos", se o resgate for "de valor consideravelmente elevado" ou o autor for "membro de bando destinado à prática reiterada de crimes contra o património, com a colaboração de pelo menos outro

membro do bando" (Art.º 204.º n.º 2 a) e g) do mesmo Código, *ex vi* Art.º 223.º n.º 3 a), sendo a segunda possibilidade muito mais provável, no contexto do *ransomware*, que a primeira.

No Brasil, ocorre um crime de *extorsão* quando a conduta se materializar em (Art.º 158.º do *Código Penal*):

> 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:
> Pena - reclusão, de quatro a dez anos, e multa.

Por sua vez, as causas de aumento de pena, aplicáveis ao *ransomware*, ocorrem quando o crime é cometido por duas ou mais pessoas, aumentando-se a pena de um terço até metade (§ 1.º do mesmo Art.º).

Sempre neste contexto, a "ameaça com mal importante", da lei portuguesa, ou a "grave ameaça", da brasileira, consiste pelo menos na possibilidade, resultante do próprio encriptamento/encriptação, de a vítima vir a perder definitivamente a disponibilidade do sistema informático e dos dados neste contidos, além das consequências adicionais que advenham da indisponibilidade temporária do sistema.

CONSIDERAÇÕES FINAIS

Depois de estes excursos, entrelaçados, cabe acrescentar que, na falta de um tipo complexo de "extorsão digital", o protocolo correspondente ao *ransomware* daria lugar a um concurso ideal de crimes, centrado no de *extorsão* em termos de unidade de ação (Art.º 30.º n.º 1, do *Código Penal* português, e Art.º 70 do *Código Penal* brasileiro).

O que fará todo o sentido quando se tratar de um acesso ilícito ao sistema informático (*ilegítimo* ou *indevido* na legislação portuguesa, *invasão de dispositivo* na brasileira) ou a uma indução em erro da vítima (*burla informática* em Portugal, *estelionato* no Brasil), seguido de um pedido de regaste, inclusive por se tratar sempre da proteção de bens jurídicos de natureza patrimonial. De fora de este concurso e pelas mesmas razões, apenas ficaria a *falsidade informática* / *falsidade ideológica*. O mesmo valendo para o encriptamento/encriptação do sistema informático, ao ser esta a via escolhida pelos criminosos para intimidar os seus titulares e os levar a pagar o resgate solicitado.

Mas já assim não será, se verificando um concurso real de crimes, quando o encriptamento/encriptação implicar uma indisponibilidade prolongada do sistema informático da qual resultem danos desproporcionadamente elevados, excedendo o nível executivo necessário à realização

da extorsão, ficando autonomamente lesado o bem jurídico protegido pela *sabotagem informática qualificada*, da legislação portuguesa, ou sejam perturbados serviços públicos essenciais à continuidade da vida social, como ocorre com a *sabotagem informática afetando infraestruturas críticas* ou o *atentado contra a segurança de utilidade pública* ou, melhor ainda, a *interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade*, respetivamente em Portugal e no Brasil.

De toda sorte e análise, estes são os apontamentos iniciais ausentes de um aprofundamento doutrinário e jurisprudencial, o que merece/merecerá análise em outro momento.

REFERÊNCIAS

CARVALHO, Américo Taipa de. "Artigo 223.º (Extorsão)" In DIAS, Jorge de Figueiredo (Dir.). **Comentário Conimbricense ao Código Penal.** *Parte Especial*. Tomo II. Coimbra: Coimbra Ed., 1999.

CAVALCANTE, Márcio André Lopes. **Comentários à lei 12.737/2012, que tipifica a invasão de dispositivo informático**. 2014. Disponível em: <http://marciocavalcante2.jusbrasil.com.br/artigos/121942716/comentarios-a-lei-12737-2012-que-tipifica-a-invasao-de-dispositivo-informatico>. Acesso em: 15 jul. 2017.

CONVENÇÃO SOBRE O CIBERCRIME. **Preâmbulo**. Budapeste, 23. XI. 2001. Disponível em: <http://www.acidi.gov.pt/_cfn/529350b642306/live/+Conven% C3%zA7%C3%A3o+sobre+o+Cibercrime++>. Acesso em: 15 jul. 2017.

COSTA, A. M. Almeida. "Artigo 221.º (Burla informática e nas comunicações)". In DIAS, Jorge de Figueiredo (Dir.). **Comentário Conimbricense ao Código Penal. Parte Especial.** Tomo II. Coimbra: Coimbra Ed., 1999.

COUNCIL OF EUROPE. **Convention on Cybercrime (CETS Nº.: 185)**. Chart of signatures and ratifications. Disponível em: <http://conventions.coe.int/Treaty/ Commun/ChercheSig.asp?NT=185&CM=1&DF=9/2/2006&CL=ENG>. Acesso em: 30 dez. 2014.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.

FREITAS, Pedro Miguel. "Breves nótulas sobre o crime de acesso ilegítimo previsto na Lei do Cibercrime". In MONTE, Mário Ferreira *et al*. (Ed.s). **Estudos em comemoração dos 20 anos da Escola de Direito da Universidade do Minho**. Coimbra: Coimbra Editora, 2014.

VENÂNCIO, Pedro Dias. **Lei do Cibercrime - Anotada e Comentada**. Coimbra: Coimbra Editora, 2011, *maxime* pp. 37-44 e 52-66;

VERDELHO, Pedro. "Lei n.º 109/2009, de 15 de Setembro, que aprova a Lei do Cibercrime (Artigos 3.º a 8.º)" In Albuquerque, Paulo Pinto de e Branco, José (Coords.). **Comentário das Lei Penais Extravagantes**, Vol. I, Lisboa: Universidade Católica Editora, 2010.

_____. "Lei n.º 67/98, de 26 de Outubro, que aprova a Lei da Protecção de Dados Pessoais (Artigos 43.º a 47.º)". In Albuquerque, Paulo Pinto de e Branco, José (Coords.). **Comentário das Lei Penais Extravagantes**, Vol. II, Lisboa: Universidade Católica Editora, 2011.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos (2a. edição): Ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2013.

WENDT, Emerson. **Internet & Direito Penal**. Risco e cultura do medo. Porto Alegre: Ed. Livraria do Advogado, 2016.

[i] Este artigo corresponde a uma ampliação, alargada ao Direito Brasileiro, da *Aula Aberta* lecionada pelo Autor Manuel David Masseno na *Summer School* do Laboratório UbiNET – Segurança Informática e Cibercrime e do MESI – Mestrado em Engenharia de Segurança Informática, do Instituto Politécnico de Beja, em Portugal, no dia 6 de julho de 2017.

[ii] WannaCry é um crypto-*ransomware* que afeta o sistema operativo Microsoft Windows e sua difusão a larga escala iniciou-se na primeira quinzena de maio de 2017, através de técnicas de *Phishing* (pescaria virtual), infectando milhares de sistemas.

[iii] Não se pretende esgotar os aspectos técnicos do protocolo de ataque *ransomware*, porém apenas analisar seu aspecto genérico.

[iv] Petya, também chamado de NotPetya ou ExPtr, é um malware do tipo *ransomware* descoberto inicialmente em 2016. Posteriormente, analistas descobriram que o *malware* evoluiu, e então está sendo tratada como um *wiper*, que tem como característica provocar destruição do acesso ao computador sem mesmo exigir um resgate, ou com pagamento, sem efeito de recuperação. Sua incidência massiva ocorreu após a incidência do WannaCry, sendo que se acreditou serem ataques semelhantes.

[v] A carteira de Bitcoins (criptomoeda) do WannaCry pode ser acompanhada pelo *link* <https://bitinfocharts.com/bitcoin/wallet/WannaCry-wallet>. Em mais de mês de ação do protocolo *ransomware* WannaCry seus autores só obtiveram cerca de U$ 130 mil de resgates (acesso em 09 de jul. 2017).

[vi] Segundo Wendt e Jorge (2013, p. 39), "O termo *phishing* é originado da palavra inglesa *fishing*, que significa pescar, ou seja, é a conduta daquele que pesca informações sobre o usuário de computador." Concepção esta, atualmente, bastante ampliada em virtude da proliferação do uso de smartphones e demais dispositivos móveis com acesso à rede.