
CYBERLAW
by CIJIC

CYBERLAW by CIJIC

EDIÇÃO N.º VIII – SETEMBRO DE 2019

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


CYBERLAW
by CIJIC

CYBERLAW by CIJIC

ISSN 2183-729

NOTAS DO EDITOR:

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

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

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

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

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

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

Será assim tão difícil perceber as diferenças?

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

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

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

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

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

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

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

- Muito Obrigado.

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

Boas leituras.

Lisboa, FDUL, 29 de Setembro de 2019

Nuno Teixeira Castro

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

CYBERLAW

by CIJIC

DOUTRINA

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

DUARTE RODRIGUES NUNES [1]

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

ABSTRACT

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

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

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

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

RESUMO

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

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

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

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

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

1.INTRODUÇÃO

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. O CONCEITO DE *RANSOMWARE*

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

44 *In www.dgsi.pt*.

45 *In www.dgsi.pt*.

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

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

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

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

4. A EXIGÊNCIA E O PAGAMENTO DO RESGATE

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

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

2 - A tentativa é punível.

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

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

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

---

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5. A EXIGÊNCIA E O PAGAMENTO DO RESGATE

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

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

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

---

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

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

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

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

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

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

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

3 - Se se verificarem os requisitos referidos:

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

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

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

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

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

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

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

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

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

6. CONCLUSÕES

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

7. BIBLIOGRAFIA

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

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

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

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

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

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

Ilegi_timo_na_Lei_da_Criminalidade_Informa_tica_e_na_CiberConvencao (acedido em 18/07/2018).

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

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

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

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

Europol – Carbanak/Cobalt Infographic, *in https://www.europol.europa.eu/pub*

lications-documents/carbanak/cobalt-infographic (acedido em 04/07/2018).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Artigos de imprensa

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

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

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

Jurisprudência

- Tribunal da Relação de Coimbra

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

- Tribunal da Relação de Lisboa

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

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

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

- Tribunal da Relação do Porto

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

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