RANSOMWARE E LGPD: UMA CONTRADIÇÃO ENTRE FINS E MEIOS EM CASO DE EXTORSÃO POR RANSOMWARE

Bruno Cardoso Lopes[1]
Felipe do Sacramento Batista[2]
Oseias Silva Moreira [3]
Caê Matos Teixeira de Almeida [4]

RESUMO:

Os avanços tecnológicos levou ao surgimento de novas modalidades delituosas em uma espécie de moldação do crime aos novos rumos tecnológicos. Nessa sentido algumas condutas criminosas que anteriormente eram praticados em ambientes fisícos passaram a ser praticados em ambientes virtuais, dificultando a identificação e punição destes, é o caso das extorsões digitais por Ransomware.

Com a globalização da tecnologia, novos direitos passaram a carecer da tutela do Estado. Dentre eles podemos observar o direito à proteção de dados, dessa maneira, visando dar mais segurança jurídica e desmarginalizar tal direito, surgiu em 2018 a Lei Geral de Proteção de Dados (LGPD), a qual após prazo de vacancia de quase 2 anos, começou a surtir efeitos em Agosto de 2021.

Contudo, muito vem se questionando se a referida Lei conseguirá atingir a finalidade pela qual fora criada e proporcionar a população em um todo a proteção aos dados, devidos aos altos números ataques por Ransomware registrado ultimamente, em especial durante o periodo pandêmico. Desta forma, o presente trabalho visa o estudo dos meios que a referida lei propociona para proteção de dados, em especial nos casos de extorsão por meio de Ransomware.

PALAVRAS CHAVES: Ransomware, LGPD, extorsão digital, sequestro de dados, cyber crimes.

---

[1] Bacharelando do curso de Direito, 10º semestre pelo Centro Universitário UNIFTC – Campus de Vitória da Conquista – Bahia. E-mail: brunoc.jus@gmail.com
[2] Bacharelando do curso de Direito, 10º semestre pelo Centro Universitário UNIFTC – Campus de Vitória da Conquista – Bahia. E-mail: fellipesb.adv@gmail.com
[3] Bacharelando do curso de Direito, 10º semestre pelo Centro Universitário UNIFTC – Campus de Vitória da Conquista – Bahia. E-mail: oseiasuesb@gmail.com
[4] Caê Matos Teixeira de Almeida, Doutorando em Filosofia do Direito na Universidad John F. Kennedy de Buenos Aires, Mestre em Direito Público pela UFBA e Pós-Graduado em Direito de Estado pela JusPodivm-Unyahna. E-mail: caemta@yahoo.com.br.

ABSTRACT:

Technological advances have led to the emergence of new criminal modalities in a kind of molding crime to new technological directions. In this sense, some criminal behaviors that were previously practiced in physical environments are now practiced in virtual environments, making their identification and punishment difficult, such as the case of digital extortion by Ransomware.

With the globalization of technology, new rights began to lack the tutelage of the State. Among them we can observe the right to data protection, in this way, to classify to give more legal security and de-maginalize such right, in 2018 the General Data Protection Law (LGPD) appeared, which after a vacancy period of almost 2 years, began taking effect in August 2021.

However, much has been questioned whether the aforementioned Law will achieve the purpose for which it was created and provide the population as a whole with data protection, due to the high numbers of attacks registered lately, especially during the pandemic period. Thus, this work aims to study the means that the aforementioned law provides to protect data, in addition to analyzing existing data and studies on the subject.

KEYWORDS: Ransomware, LGPD, digital extortion, data hijacking, cyber crimes.

Introdução

A vida das pessoas, hoje em dia, parece cada vez mais atrelada aos mecanismos virtuais. Porquanto, a coleta de dados pessoais é serviço indispensável para as empresas em todo o mundo. Os serviços oferecidos pelas entidades públicas e privadas são, certamente, facilitados pelos sistemas de informações que armazenam os dados de seu público. É por essa perspectiva que, cada vez mais frequente, ocorrem os crimes virtuais que disseminam a violação da privacidade e da intimidade das pessoas.

Com o dito, o Ransomware [5] é um dos principais meios de invasão de dados que existe no mundo. Através dele, os criminosos bloqueiam os acessos dos sistemas de uma empresa e cobram, em criptomoedas, o resgate para retorno funcional do acesso. O reconhecimento dos criminosos não é uma tarefa fácil, visto que eles possuem preparação técnica para impedir que sejam localizados e consequentemente apreendidos.

[5] Os ataques Ransomware são modalidades de invasão que visa criptografar dados e arquivos pessoais. O Locker ransoware, por sua vez, é projetado para bloquear o computador, impedindo que as vítimas o utilizem. Esse tipo de software, implica na extorsão por criminosos usando o bloqueio de dados em empresas, exigindo para o reestabelecimento de acesso, o pagamento de resgate. (CARPEGGIANI, Markus de Lema. FREITAS, Marcio. Ataques Ransomware. 2005. 5° seminário de tecnologia, gestão e educação. III jornada acadêmica & simpósios de Egressos. Faculdade Alcides Maya e escola técnica)

Em razão do aumento desse tipo de crime, a preocupação com uma solução adequada para sanar esse tipo de invasão vem crescendo em todo mundo. No Brasil, a Constituição Federal de 1988 protege a inviolabilidade à vida privada e a intimidade quando dispõe em seu artigo 5º, inciso X, assegurando o direito a indenização pelos danos em caso de sua violação.

Percebe-se, no entanto, a insuficiência preventiva e punitiva do disposto na Magna Carta quanto aos crimes virtuais. A sociedade contemporânea precisa adequar a legislação à medida que os crimes evoluem, com isso, foi criada no ano de 2018 a lei intitulada de LGPD (Lei Geral de Proteção de dados). A lei que entrou em vigor em setembro de 2020 visa a proteção dos dados estabelecendo as diretrizes necessárias em relação a coleta e processamento de dados em instituições privadas e públicas, ou seja, União, Distrito Federal, Estados e Municípios devem seguir as imposições legais sob o risco de consequente sanção caso não sigam as diretrizes culminadas no corpo da lei. A questão, no entanto, é a contradição existente nos números sancionais e de adequação à lei e os quantitativos exigidos pelos criminosos, sob a lógica dos prejuízos financeiros das empresas afetadas.

2. LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

Os crimes virtuais são, sem dúvidas, um problema a ser combatido no século XXI. A intimidade e vida privada dos usuários de serviços virtuais estão cada vez mais vulneráveis aos ataques feitos por desconhecidos com capacidade técnica de obscurecer sua identificação. Existem, por essa questão, uma dupla preocupação, pois, lado a lado com os usuários estão as empresas que trabalham e precisam armazenar os dados dos seus clientes. A saber, a exposição dos dados armazenados viola a privacidade do particular e traz sérias consequências financeiras e ética às empresas vítimas desses crimes.

Países como a Alemanha já haviam na década de 80 reconhecido a autoderminação informativa[6] como direito fundamental. Com isso, ao indivíduo é facultado a decisão sobre dispor ou não de seus dados pessoais para armazenamento em sistemas empresariais. O sigilo às informações é visto como fundamento necessário para preservação da intimidade do indivíduo. Samuel Warren, tratou, nos anos 1890 do direito

[6] A autodeterminação informativa é o poder que cada cidadão tem sobre seus próprios dados pessoais. Isso significa que, em determinadas circunstâncias, ou seja, quando a pessoa puder fazer essa escolha, ela pode decidir se seus dados serão coletados, tratados, compartilhados. (PRIVACY TOOLS. 2021)

à privacidade. Ao notar o ano da escrita de Warren, percebe-se uma preocupação juvenil com as questões da privacidade e intimidade social, essa preocupação evoluiu à medida que foram evoluindo a tecnologia mundial. As leis que antes pareciam ser suficientes para combater os males tecnológicos precisaram de um olhar mais rigoroso frente a ampliação dos malefícios ocasionados por criminosos virtuais. Ricardo Villas Boa Cueva, reitera:

> "O rápido desenvolvimento da informática, contudo, multiplicou as possibilidades de invasão da intimidade. A ubiquidade dos meios eletrônicos de coleta e troca de informações permite que se recolham informações virtualmente sobre todas as atividades cotidianas, afim de organizá-las em categorias de comportamento, de preferências, de crenças, de consumo, entre outras, e assim traçar perfis de personalidade voltados para o exercício de alguma modalidade de controle social, político, econômico ou mesmo existencial sobre os indivíduos." (CUEVA. 2016. p.8)

Com isso, nota-se que, como discorre Cueva, com o desenvolvimento informático ocorre, também, o desenvolvimento da invasão a intimidade. A necessidade de armazenamento de informações particulares parece um prato cheio para as atividades ilícitas dos criminosos virtuais. Para acompanhar o desenvolvimento social e suas tecnologias, se faz necessário, como já dito antes, o desenvolvimento e acompanhamento das leis com rigor tamanho à gravidade dos crimes praticados virtualmente. Como visto, a constituição Federal de 1988, protege a vida privada e intimidade das pessoas, ocorre que, com a insuficiência punitiva, tendo em vista a gravidade dos crimes em comento, fez necessário a criação de uma lei especial para tratativa exclusiva da proteção dos dados pessoais dos brasileiros.

A LGPD trouxe exigências a serem cumpridas por empresas brasileiras quanto as diretrizes de armazenamento de dados. A lei exposta, veio como um complemento de normas que já impunham obrigações aos responsáveis pelos dados de seus clientes, pois, sobre a mesma tratativa já disciplinavam o código do consumidor no que se refere ao banco de dados e cadastros de consumidores, e as leis 12.414/11 e 12.527/11 que tratam do cadastro positivo e o acesso as informações públicas. Ocorre, porém, que a proteção aos dados pessoais já existentes, importam lacunas que precisam ser preenchidas. Não dar para tratar da proteção de dados sob a limitação, exclusivamente, das leis consumeiras e jurisprudências restritivas. Com isso, a criação da LGPD trouxe esperança de mais segurança e proteção dos usuários de serviços virtuais.

A lei acompanha os cidadãos em todos as esferas de suas vidas, com isso, a LGPD legisla a proteção de um público cujo vida privada caminha por uma linha tênue junto as más intenções de criminosos. Os anseios da Lei Geral de proteção de dados parecem realmente inclinados ao combate dos crimes virtuais, o que torna sua vigência extremamente necessária, pois, ao fazer uma análise da sociedade moderna, percebe-se que a necessidade social de acompanhar as facilidades tecnológicas tem sido cada vez mais frequente. O fazer online tomou conta dos aparelhos eletrônicos dos cidadãos, e isso, não se trata de um maleficio, mas, de uma eficiência evolutiva ao longo do tempo. Os mercados não tem mais filas, os bancos não são mais tão cansativos e as escolas passaram a ser, também, virtuais. Percebendo, a evolução digital está cada vez maior e isso não deveria ser um problema, porém, todo esse acesso simplificado tem tornado frágil o cruzamento de dados do público usuário. Nesse sentido, discorre Goulart;

> "Por meio do intenso cruzamento e processamento de dados pessoais criam-se perfis de cada um dos usuários, em uma atividade chamada de profiling. Com isso, cada tipo de perfil receberá resultados personalizados que levam em conta uma serie de aspectos identificados. Com tais informações, além do conteúdo ser personalizado há também a personalização da propaganda." (GOULART, 2014. p.95)

Com o exposto por Goulart, percebe-se o risco social enfrentado em decorrência da exposição de dados nos meios virtuais. As leis são uma esperança para que esses riscos sejam reduzidos. A efetividade das disposições já existentes no Brasil, não preenchia os espaços que deveriam para combate e punição dos agentes criminosos. A partir de agosto de 2020, a LGPD vigorou para atender o público de todo o país e estrangeiros que estiverem no território. A lei 13.709 regulamenta a proteção de dados pessoais com o fim de resguardar a privacidade e a intimidade das pessoas. A norma trouxe uma segurança jurídica para os usuários dos serviços virtuais. Sua disciplina resguarda todo tipo de público, dando atenção, também, ao público considerado mais frágil, como a criança e ao adolescente e os considerados sensíveis, imputando sanções para aquelas organizações que não se adequarem aos mandamentos da norma.

O artigo 3° da Lei LGPD, evidencia o rigor pretendido pela lei;

> "Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
>
> I - A o-peração de tratamento seja realizada no território nacional;"

Nota-se que a lei em comento não será aplicada apenas quando o ilícito por praticado dentro do território brasileiro. Assim, estende-se sua eficácia ao local onde houver acontecido o acesso ilegal de dados, sobre isso Tomasevicius Filho já havia comentado em 206.

> "Na tentativa de frear violações de privacidade por meio de coleta , armazenamento e tratamento de registros , dados pessoais ou comunicações por meio do art. 11, caput, §§, 1° e 2°, estabeleceu-se que o marco civil da internet se aplica quando, pelo menos um dos atos realiza-se no Brasil ou quando um dos terminais estiver no Brasil e que pessoas jurídicas com sede no exterior devem sujeitar-se a lei brasileira quando tiverem , pelo menos, uma integrante do mesmo grupo econômico com estabelecimento no Brasil. A despeito da boa intenção, a violação pode não acontecer no Brasil, mas poderá acontecer na outra ponta de transmissão de dados no exterior." (TOMASEVICIUS FILHO, 2016. p.277)

Com o dito, perceber-se-á que houve grande inovação pós palavras de Tomasevicius, pois, com a vigência da Lei geral de Proteção de Dados, os crimes de divulgação de dados, ainda que cometidos no exterior serão igualmente punidos como se estivessem acontecido no Brasil, ainda que a empresa brasileira não tenha sede em território nacional.

Vale ressaltar que, a LGPD proíbe a autorização do fornecimento dos dados pessoais pelo Estado, a partir dela, somente o titular poderá escolher entre dispor ou não de seus dados pessoais. Esse avanço traz conforto aos direitos fundamentais dos cidadãos, pois dá ao indivíduo o poder de decisão sobre suas próprias informações. Com o visto, nota-se a amplitude da proteção da lei ao atingir pontos que antes não era possível. Com o advento da lei, os brasileiros que são um dos povos mais vulneráveis aos ataques digitais, poderá ter um pouco mais de confiança de que seus dados lançados nos sistemas operacionais estejam, de fato, protegidos.

Assim, percebe-se a que a criação da lei LGPD instituiu um crescimento necessário quanto a tratativa de segurança e direito à privacidade do público brasileiro. Não é dizer que não existiam normas que tratassem do assunto, pois, a pioneira nesse assunto foi a Constituição Federal de 1988. Ocorre que ao adentrar a esfera do desenvolvimento tecnológico, também se adentra as ambições criminosas por trás das telas. Assim, quanto mais os crimes virtuais crescem, mais carece de uma lei com rigor suficiente para pará-los e puni-los.

3. RANSOMWARE E EXTORSÃO POR MEIO ELETRÔNICO

Como visto nas motivações que levaram a criação da lei LGPD, os principais destaques, dizem respeito à a crescente invasão de dados por meios eletrônicos. Dentre esses ataques o mais temido e mais usado pelos criminosos nos últimos tempos são os ataques *ransomware*. O *ransomware* funciona através do bloqueio de dados de um determinado servidor, com isso, os agentes criminosos pedem um resgate para liberação do acesso. Essa ação tem dado prejuízo a pessoas e empresas em todo mundo, com isso, os ataques ransomware se transformou em um vírus entre os hackers espalhados pelo planeta. A possibilidade de ganhar muito dinheiro através dos resgates é o principal instigador na mente desses personagens. O problema, para além dos valores pagos nos resgates, é saber se após pagar os valores solicitados pelos criminosos, o acesso será realmente restabelecido, pois, não há nenhuma garantia de que eles realmente cumpram com o dito. Em alguns casos, os agentes criminosos, não devolvem o acesso, e, ainda pedem um segundo resgate para liberação dos dados.

As incertezas quanto à possiblidade de não haver de volta o controle dos bancos de dados, faz com que muitas vítimas não paguem o valor solicitado, muito embora, de qualquer modo, estão sujeitos ao prejuízo. Richardson e North reiteram;

> "Tanto indivíduos quanto empresas enfrentam a decisão de pagar quando não tem backups adequados para se recuperar do ransomware. Como tal, a decisão se resume a duas questões relacionadas. Em primeiro lugar, os dados valem mais do que o resgate? E, em caso afirmativo, qual é o nível de confiança de que o criminoso de que o criminoso irá descriptografar os dados se o resgate for pago. (RICHARDSON, NORTH. 2017. P.1)

A questão enfatizada no trecho citado é realmente um ponto a ser questionando. O prejuízo não viria de qualquer modo? Algumas empresas se submetem a chantagem dos criminosos, porém algumas pensam sobre as consequências que advirão da submissão aos chantagistas. Ao pagar o que está sendo cobrado, o ato poderá fazer com que os agentes se sintam confiantes para agir em uma segunda e até mesmo uma terceira vez contra a mesma empresa, além, é claro, de que os criminosos atuam em grupo, e certamente passarão as informações para outros comparsas que se sentirão confortáveis de aplicarem o mesmo golpe.

A compreender, há nesses ataques uma evolução quanto ao seu modo de operação, se por um lado as empresas de segurança aumentam para prevenir a ação dos criminosos,

por outro, os criminosos sofisticam suas operações de maneira a não deixar rastros do feito. A ransomware já evoluiu para várias plataformas digitais, com isso, há uma preocupação maior quanto o controle e prevenção desse tipo de crime, pois, parece que não há, ainda, um modo de operação que os intimide.

A evolução tecnológica que faz com que os cidadãos utilizem as plataformas digitais para fazer suas atividades, é a mesma evolução que aprimora o agir dos criminosos virtuais. Assim, as pessoas e empresas vivem cada vez mais assustados com esse tipo de crime. Não há, aparentemente, um feito que as empresas podem fazer por sua segurança virtual que os ransomware também não possam fazer. A habilidade deles, é exatamente o agir por trás das telas.

Os ataques ransomware tiverem um crescimento considerável no ano de 2020. A crise pandêmica ocorrida no ano citado parece ter sido o principal motivo do aumento dos crimes virtuais. A saber, a vida dos cidadãos teve que se adequar ao mundo digital, por essa razão, o que parecia já ser feito, preferencialmente, através das telas, passou a ser uma obrigatoriedade. Com isso as ameaças digitais crescerem e se transformaram no terror de muitas pessoas e categorias empresariais. A pandemia do coronavirus fez com que bancos criassem aplicativos de pagamentos, algo que além de ser novo, precisaria entrar em funcionamento o mais rápido possível, além é claro, dos pagamentos e compras que passaram ser virtualmente. Toda essa adaptação trouxe para os agentes criminosos um prato cheio para que pudessem extorquir suas vítimas, que sem outra alternativa, tiveram que aderir as normas de prevenção do novo vírus. (MIRANDA E PEREIRA. 2021. P68)

Muitas empresas brasileiras foram afetadas pelo ransomware em 2020, e ao que parece, continuarão sendo vítimas em 2021. A pandemia apesar de estar um momento mais ameno, ainda faz com que as atividades dos brasileiros sejam, em sua maioria, feitas virtualmente. A solução para esses ataques parece um pouco distante, devido a capacidade evolutiva dos ransomware. A solução mais eficaz seria a punição adequada para os criminosos por traz da tela, porém, até mesmo a identificação dos agentes é algo distante da realidade, pois, os mesmos possuem mecanismos para não serem identificados. Nesse sentindo Savage Coogan e Lau, reiteram:

> "À medida que o mundo muda para a internet das coisas (IoT[7]), não há dúvida de que o ransomware também mudará para a IoT. Embora isso possa parecer rebuscado no início, os pesquisadores já conseguiram assumir o controle dos sistemas de um Jeep Cherokee em movimento, se os pesquisadores podem fazer isso, o ransomware também pode." (SAVAGE, COOGAN & LAU. 2015. P.37)

Assim, como visto nas palavras acima, se torna cada vez mais difícil o controle sobre os ransomware, pois eles se aprimoram com a evolução tecnológica.

4. RANSOMWARE E LEI GERAL DE PROTEÇÃO DE DADOS

A partir da exposição da finalidade da Lei Geral de Proteção de dados e os crescentes ataques Ransomware, pode-se afirmar que a lei foi de extrema necessidade para segurança jurídica dos milhões de usuários da tecnologia. Ocorre que, em relação aos ataques listados, as empresas são as mais afetadas pelos crimes, e, ao que consta, a finalidade da lei LGPD é tratar justamente dos crimes cometidos na esfera administrativa, ou seja, a lei não se ocupa dos casos envolvendo o particular e atividades sem fins lucrativos. Por essa vertente, a lei tratou da adequação de empresas nacionais que estejam situadas no Brasil ou no estrangeiro.

A adequação das empresas a nova lei em comento, foi, e é, o maior desafio para fazer cumprir as exigências da norma. Ocorre que, o aparato financeiro envolvido custa valores altíssimos aos cofres empresariais. Antes, a preocupação do mercado era basicamente encontrar meios internos para prevenção dos ataques ransomware, porém, com o advento da lei, a preocupação para a adequação se tornou caso de obrigatoriedade sob pena de arcar com as sanções expostas na norma vigente. William Faria, reforça:

> "Com a entrada em vigor da Lei Geral de Proteção de Dados (LGPD) no mês de setembro, as atenções das empresas ficaram voltadas para os processos de adequação à lei. Porém, muitas se esquecem de que para obter a real Proteção de Dados Pessoais, é necessário um forte mecanismo de segurança da informação, principalmente quando falamos de ataques de ransomware." (Faria. 2020. p.1)

[7] A Internet das Coisas (**IoT**) descreve a rede de — "objetos físicos" — incorporados a sensores, software e outras tecnologias com o objetivo de conectar e trocar dados com outros dispositivos e sistemas pela internet. Esses dispositivos variam de objetos domésticos comuns a ferramentas industriais sofisticadas. (ORACLE BRASIL. O que é a IoT? 2020)

Os mecanismos de segurança expostos por Faria no trecho acima ilustram a realidade de investimentos que a lei acarreta aos agentes de tratamento de dados. Não há margem para discursão a respeito da necessidade da lei, todavia existem brechas claras a respeito das sanções impostas pela norma em comparação com um possível pagamento de resgate, ou até mesmo arcar com as consequências quando, e se, os dados dos clientes forem expostos de alguma maneira. Nota-se que a Lei 13.709 foca sua atenção na adequação das organizações às normas. Ocorre que, o público a que ela se direciona, sente-se preso ao que se pode chamar de "beco sem saída", pois, a questão econômica que é o que move os países em geral, resta afetada de qualquer maneira.

Assim, os serviços de adequação custam caro aos cofres empresariais e, a não adequação aos serviços de segurança leva as empresas a pagarem multas significativas, ao mesmo passo que, o não pagamento do resgate aos criminosos, não sairá barato. As sanções dispostas pela LGPD estão dispostas em seu artigo 52 e consistem em advertência, multa simples, multa diária, publicização da infração, bloqueio dos dados pessoais e até mesmo na eliminação dos dados pessoais a que se refere a infração.

Pensando, a aplicação da lei de a proteção de dados impostas aos agentes de tratamento certamente não traduz a realidade vivenciada no atual cenário brasileiro. Ao analisar os ataques ransomware, tem-se visto que eles atingem até mesmo os que se intitulam mais preparados. A responsabilização das organizações quando do vazamento de dados por ataques ransomware, tem gerado discursões entre as entidades afetadas, afinal de contas, existe um dilema que dificulta a adequação na forma exigida pela lei.

O artigo 43 da LGPD dispõe sobre as excludentes de responsabilidade dos agentes de tratamento de dados, que ocorrem quando provarem que a) não realizaram o tratamento de dados pessoais que lhes é atribuido; b) quando não houver violação à LGDP mesmo realizando o tratamento dos dados pessoais que lhes é atribuido e c) por culpa exclusiva do titular dos dados ou de terceiro.

A segunda excludente de responsabilidade presente no artigo 43 da LGPD merece especial atenção, pois dispõe que em caso de culpa exclusiva de terceiros os agentes de tratamento não pagarão as sanções impostas. Ocorre, todavia, que não se pode determinar, com certeza e segurança suficientes quando a culpa será exclusivamente de terceiro, pois, os ataques ransomware invadem até mesmos os mais preparados e mais sofisticados sistemas de segurança. A saber, até mesmo o Estado se tornou vulnerável aos ataques dos cibercriminosos. Alguns órgãos do poder judiciário como, o Superior Tribunal de Justiça, o tesouro nacional e outros, foram afetados por esse tipo de ataque. A questão é; se até

mesmo aqueles que tratam das leis não conseguem prevenir e combater os ataques, como uma organização empresarial comum poderia superar os sistemas de segurança do Estado?

A culpa exclusiva descrita no corpo da lei parece ser o único jeito de isentar as organizações de arcar com os altos custos das sanções, mas, na prática, não se consegue mencionar quando a culpa foi exclusiva de um terceiro, pois com a evolução dos ataques ransomware, não dar para dizer qual é o limite máximo de segurança que poderia detê-los. Os ataques ao Tribunal de Justiça exemplificam bem essa problemática, pois, sendo ele um órgão estadual, certamente possui a mais evoluída tecnologia para prevenir esse tipo de crime. No entanto, foram vítimas dos cibercriminosos.

Há, decerto, uma preocupação quanto a tratativa da lei LGPD, pois, considerando o nível de segurança que seria necessário para deter os ataques ransomware, pode-se dizer que não haveria mecanismos suficientes para combatê-los. Os ataques virtuais não são um ato paralisado no tempo, suas técnicas se adequam, evoluem e aprimoram. É o mesmo observar que se possa ter a respeito da própria tecnologia. Há 10 anos não era possível fazer muitas coisas que a tecnologia possibilita nos dias atuais. O mesmo se pode pensar em relação aos crimes virtuais, cada dia que passa eles encontram uma forma evolutiva de extorquir as pessoas e organizações por todo o mundo. Pensando, não seria possível que os agentes de tratamento se adequem de maneira satisfatória de modo a prevenir qualquer ataque virtual, pois, se os cibercriminosos evoluem suas técnicas ilícitas, pará-los, definitivamente seria um feito quase impossível.

5. INEXIGIBILIDADE DE CONDUTA DIVERSA E PAGAMENTO DE "RESGATE DE DADOS" EM CASOS DE RANSOMWARE

A conduta dos detentores dos dados diante dos casos de sequestro de dados por Ransomware carece de atenção especial. Isso porque essas empresas são colocadas em situações delicadas onde devem ponderar entre o pagamento para resgatar os dados ou não ceder a extorsão, e, consequentemente, terem seus dados violados e perdidos, além de suportar os ônus decorrentes dessa violação.

Por oportuno, Fábio Lucena de Araújo, observa que cabe ser feita uma análise sobre a extensão do dano sofrido. De forma que, se a vítima possuir dados importantes que venham a trazer altos prejuízos a si quanto a terceiros, talvez a melhor opção seja pagar o resgate, mesmo contrariando as orientações dos órgãos de segurança pública que recomendam não pagar. (ARAUJO, 2021.)

Em contrapartida, como dito anteriormente, mesmo com o pagamento do resgate não há garantia de recuperação de todos os dados violados. É o que apontou um recente estudo realizado pela empresa de tecnologia de segurança cibernética Cybereason[8], o qual constatou das empresas que pagaram o resgate dos dados: a) 46% indicaram que recuperaram o acesso, com alguns ou todos os dados corrompidos, após realizar o pagamento: b) 51% recuperaram com sucesso o acesso aos dados criptografados sem qualquer perda de dados: c) 3% indicaram que não recuperaram o acesso a nenhum dos dados criptografados e: d) 80% incorreram em outro ataque.

Os autores Allan Liska e Timothy Gallo, trazem uma abordagem necessária quanto a realização ou não do pagamento do resgate dos dados, a qual merece destaque. Vejamos:

> "Para ser honesto, gostaria de dizer "NÃO" com uma fonte de 350 pontos em negrito. Contudo, essa é uma resposta demasiadamente simples. É possível que você tenha arquivos que sejam simplesmente imprescindíveis no sistema criptografado, que você não tenha feito backup desses arquivos e não disponha de nenhum método para recriá-los – ou, se houver alguma vida humana correndo riscos iminentes. Talvez você considere efetuar o pagamento. Outro aspecto a ser observado é o fato de que os autores de ransomware tendem a conhecer a distribuição demográfica de seus alvos e escolham pontos cujos preços sejam apropriadamente baixos para incentivar o pagamento, e esses preços se compariam de modo geral aos custos da restauração dos dados." (2017, p. 27)

Conclui-se do trecho acima que, em alguns casos, as vítimas dos ataques ransomware, não tem outra alternativa senão fazer o pagamento do resgate, pois precisam proteger um bem maior, muitas vezes, suas próprias vidas ou integridade física.

Por essa razão, essa conduta criminosa tem acompanhado a evolução tecnológica, e tem dificultado a vida das organizações empresariais brasileiras. O resultado disso é que o Brasil é um dos países com maior incidência desse tipo de crime, segundo a pesquisa da empresa de soluções de segurança de rede Sonic Wall[8], o país ocupa a quinta posição no ranking mundial e a primeira dentre os países da América do Sul dos países que mais sofreram tentativas de ataques por Ransomware no mundo em 2021. A referida pesquisa

[8] A Cybereason oferece prevenção, detecção e resposta de endpoints e monitoramento ativo. A Cybereason, criadora da principal plataforma de defesa cibernética, devolve a vantagem ao defensor por meio de uma abordagem completamente nova à segurança cibernética. (COPYRIGHT © NEC LATIN AMERICA S.A. 2021)

[8] A SonicWall,é uma empresa fabricante de soluções de segurança abrangente que inclui Segurança de rede, Segurança móvel, VPN segura, Segurança de e-mail, Conformidade com PCI-DSS, Voz sobre IP (VoIP) e Segurança virtual. (© 2021 SONICWALL. ALL RIGHTS RESERVED.)

indicou que o país somou, no primeiro semestre do referido ano, o total de 9.116,409 (nove milhões, cento e dezesseis mil e quatrocentos e nove) ataques.

As extorsões digitais ocorrem através do pedido de resgate que, como já dito antes, acontecem, geralmente, com exigência de pagamento em moedas virtuais. Os alvos dos criminosos, geralmente, definem que tipo de ataque aplicar. Assim, o ransomware pode complicar a extorsão de acordo com possibilidade financeira de suas vítimas, quanto maior for a capacidade financeira, maior será o valor cobrado pelos agentes para liberação dos dados sequestrados. Fábio Lucena de Araújo, reitera:

> "Existem ataques mais simples e outros mais complexos, estes ocorrem quando existe um alvo específico, seja pessoa física, pessoa jurídica de direito privado ou até mesmo de direito público. As abordagens se desenvolvem de diversas formas, seja explorando as falhas dos sistemas ou também por meio de engenharia social, explorando as nossas vulnerabilidades sociais" (ARAÚJO. 2019. P.95)

Com isso, as vulnerabilidades sociais narradas por Araújo retratam, de certo, o empreendimento das empresas vítimas. Os criminosos virtuais tratam de estudar todas questões que possam lhes favorecer, e por muitas vezes compartilham informações com outros que, com igual má-fé, extorquem aqueles que já foram extorquidos.

Como já dito, antes da entrada em vigor da Lei 13.709/18, já haviam outros institutos que tratavam das questões de crimes virtuais. O Código Penal ocupou-se em seu artigo 153, § 1°, da questão da divulgação de dados pessoais sem justa causa:

> Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem:
> Pena - detenção, de um a seis meses, ou multa, de trezentos mil réis a dois contos de réis. (Vide Lei nº 7.209, de 1984)
> § 1 o -A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: (Incluído pela Lei nº 9.983, de 2000)
> Pena - detenção, de 1 (um) a 4 (quatro) anos, e multa. (Incluído pela Lei nº 9.983, de 2000).

Assim como na disposição para punição da exposição de dados dada pelo código penal, e observando a questão coercitiva dada pelos criminosos às vitimas de seus crimes,

pode-se dizer que as organizações vítimas das extorsões ransomware podem se valer, também, do artigo 22 do mesmo código que dispõe:

> "Art. 22 - Se o fato é cometido sob coação irresistível ou em estrita obediência a ordem, não manifestamente ilegal, de superior hierárquico, só é punível o autor da coação ou da ordem. (Redação dada pela Lei nº 7.209, de 11.7.1984)"

Analisando as perdas e ganhos que os agentes de tratamento estão sujeitos ao serem chantageados através dos ransomware, pode-se afirmar que não há ganhos, somente perdas. Ao virarem alvo dos crimes virtuais, as organizações estarão sujeitas a prejuízos financeiros, além de incertezas sobre se realmente os cibercriminosos devolverão os dados sequestrados e, ainda, a reputação empresarial poderá sofrer descredibilidade. Com isso, compreendendo a lei 13.709/18, em relação as sanções aplicadas aos agentes de tratamento e, analisando o artigo 22 do Código Penal brasileiro, pode-se afirmar que, ao realizarem o pagamento do resgate, as empresas agem sob inexigibilidade de conduta diversa, pois naquele momento não havia outra alternativa senão ceder ao pagamento do valor pretendido. A tratativa desse ponto é muito mais sobre estar de mãos atadas do que se adequar os mandamentos da lei. Outrossim, por lógica, é bem mais provável a devolução dos dados sequestrados quando do pagamento, do que, da recusa dele.

Entendendo a escrita acima, não é que as vítimas devem ceder a chantagem dos criminosos, mas sim, fazer entender que muitas vezes as empresas se veem coagidas pelas sanções legislativas e pelas consequências advindas do não pagamento do resgate pretendido pelos criminosos.

6. CONSIDERAÇÕES FINAIS

Por todo o visto conclui-se que, as normas brasileiras ainda precisam se adequar a evolução tecnológica com coerência e eficácia. Não se pode negar que houve evolução, afinal, como dito no corpo do texto, hoje contamos com normas que não existiam há algum tempo atrás. O reconhecimento de que a Lei Geral de Proteção dados é de verdade essencial, não faz com que desprezemos as lacunas e contradições existentes nela. A lei veio em um momento em que a vida dos brasileiros, pessoas jurídicas e privadas, passavam por uma situação delicada. A vigência da lei que veio a partir de 2020, praticamente nasceu junto com o início da pandemia do Corona vírus. Nesse cenário, a

população mundial estava submetida a adaptações de fazer praticamente tudo virtualmente e com essa nova realidade despertou ainda mais os anseios dos ciberciriminosos, levando as organizações empresariais e os particulares a ficarem mais suscetíveis às novas técnicas de extorsão por meio do sequestro de dados.

Com o exposto, entende-se que a Lei 13.709/18, criada em consonância com a Constituição Federal, trouxe a segurança jurídica que pretendia em relação a criação, por parte dos agentes de tratamento, da instalação de equipamentos de segurança, todavia, havendo inexigibilidade de conduta diversa, a lei peca em relação a sanção, pois não devem serem punidos aqueles que não podem agir de outra maneira. Ora, se os cibercriminosos usam a tecnologia para cometer os intentos criminosos, não evoluiriam eles junto com a tecnologia? Esse é o ponto. A legislação, sob o olhar da coerência, não poderia imputar a uma organização uma punição tão severa a algo que nem ela mesmo tem controle. Se contarmos os ataques ocorridos aos órgãos do Estado, podemos concluir que, de fato, não há, ainda, segurança capaz de deter completamente as ações dos criminosos virtuais.

Para além da questão da segurança quase impossível de existir, pode-se citar também, outra contradição quanto aos valores cobrados pela ANPD[9], pois, quando uma organização não se adequa as disposições impostas pela lei, ela terá que pagar uma multa, aquela do artigo 52 da LGPD. Porém, os valores muitas vezes ultrapassam até mesmo os valores exigidos nos resgates. Então, dessa maneira, não seria melhor pagar o que pedem os criminosos? Parece que as lacunas existentes na lei impossibilitam que as organizações a que ela se direciona se sinta confiante em sua legislação.

Por fim, a lei é de fato necessária e veio no melhor momento, mas, precisa se adequar as necessidades dos agentes de tratamento, fazendo com que eles se sintam amparados pela segurança oferecida pela legislação. Ademais, a adequação de segurança imposta pela lei parece falha até mesmo para o próprio Estado, pois, sua segurança digital, não foi capaz de conter os ataques que alguns de seus órgãos foram vítimas. A lei é indispensável para o bom funcionamento da ordem, mas, precisa ser eficaz quanto aos interesses e a realidade social.

Referências

[9] Autoridade Nacional de Proteção de Dados.

ARAUJO, F. **Aspectos Jurídicos no Combate e Prevenção ao Ransomware**. Revista do Ministério Público do Estado do Rio de Janeiro nº 71, jan./mar. 2019, p. 93 - 118. Disponível em : http://www.mprj.mp.br/servicos/revista-do-mp/revista-75. Acesso em novembro. 2021.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília: Senado, 1988.

BRASIL. Decreto Lei n° 13.709, de 14 de agosto de 2018. Planalto. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm . Acesso em out. 2021.

COPYRIGHT. NEC Latin America S.A. NEC e Cybereason assinam acordo para fornecer soluções avançadas de segurança cibernética ao mercado brasileiro. 2021. Disponível em https://br.nec.com/pt_BR/press/PR/20191211054740_4154.html . Acesso em nov. 2021.

COPYRIGHT. Sonic Wall. Explore os principais motivos que estão fazendo as empresas se mobilizarem para o "novo normal" dos negócios e libertarem-se das restrições do passado. Disponível em https://br.nec.com/pt_BR/press/PR/20191211054740_4154.html . Acesso em nov. 2021

CUEVA, Ricardo Villas Boas**. A insuficiente Proteção de Dados no Brasil**. Capa, Justiça e Cidadania. Revista de Direito Civil Contemporâneo. Vol. 13. São Paulo. Novembro de 2019. Disponível em: file:///C:/Users/HOME/Downloads/guialcantara-a-insuficiente-proteo-de-dados-pessoas-no-brasil.pdf . Acesso em out. 2021.

Decreto-Lei 2.848, de 07 de dezembro de 1940. **Código Penal**. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940.

FARIA, William. Ransomware e a LGPD: **pagar o sequestrador ou tomar multa da ANPD?** Computerword – Itmídia. 2020. Disponível em: https://computerworld.com.br/seguranca/ransomware-e-a-lgpd-pagar-o-sequestrador-ou-tomar-multa-da-anpd/ **.** Acesso em out. 2021.

GOULART, Guilherme Damásio**. Condicionando, Liberdade e Privacidade: Compreendendo as novas tecnologias por meio do admirável mundo novo**. Revista Diálogos do Direito, v.4, n. 6, julho de 2014. Disponível em: http://ojs.cesuca.edu.br/index.php/dialogosdodireito/article/view/580. Acesso em 29 de out. 2021.

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

NEVES, Lucas Miranda. PEREIRA, Nicholas de Lucas Bastos**. Ransomware e Phishing Durante a Pandemia de Covid-19.** Revista tecnológica da Fatec Americana, Vol. O9, n. 01,

ORACLE BRASIL. Gerenciamento de Cadeia de Suprimentos. **Internet das Coisas**. O que é IoT? 2020. Disponível em: https://www.oracle.com/br/internet-of-things/what-is-iot/ . Acesso em out. 2021.

RICHARDSON, Ronny – North, Max M. Ransomware**: Evolution, Mitigation and Prevention**. Disponível em: https://digitalcommons.kennesaw.edu/facpubs/4276/ . Acesso em out. 2021.

SAVAGE, Kevin – COOGAN, Peter, & Lau, Hon. **The evolution of ransomware: Symantec.** Version 1.0 – 2015. Disponível em: htt://slidlegend.com/the-evolution-of-ransomware-Symantec-59b322f117223dd6c7341e7f4.html. Acesso em out. 2021.

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: **Uma Lei sem Conteúdo normativo**. Estudos Avançados. São Paulo – SP, V. 30, n.86, 269-285, 2016. Disponível em: https:/wwwrevsitas.usp.br /eav/article/view/115093. Acesso em 29 de outubro. 2021.

TOOLS Privacv. Autodeterminação informativa: você conhece esse conceito? Privacv Tools 2021. Disponível em: https://www.privacytools.com.br/autodeterminacao-informativa/ . Acesso em nov. 2021.

UNIFTC

ORIENTAÇÃO DE TRABALHO DE CONCLUSÃO DE CURSO

TERMO DE COMPROMISSO

CARTA DE APROVAÇÃO DO ORIENTADOR PARA ENTREGA DO TRABALHO DE CONCLUSÃO DE CURSO

Vitória da Conquista - BA, 22 de Novembro de 2021

Eu Prof. Caê Matos Teixeira de Almeida do colegiado de Direito

após analisado e corrigidos dos discentes matriculados no curso de Direito, **concordo com a entrega** do seu Trabalho de Conclusão de Curso (TCC) intitulado: Barramuare e [illegible] contradição entre fins e meios em caso de extorsão por barramuare.

Declaro pelo presente instrumento estar de acordo com o trabalho aqui apresentado e ciente das normas que regem o TCC no Regulamento Discente – Trabalho de Conclusão de Curso de Direito (TCC) 2021.2 – UniFTC, divulgado por esta Unidade de Ensino, bem como a disponibilização em formato pdf, em sua versão final, para o Repósitorio Institucional (RI).

Discentes: Bruno Cardoso Lopes e-mail: brunoc.jus@gmail.com

Discentes: Fellipe do Sacramento Batista e-mail: felipesb.adv@gmail.com

Discentes: Ozias Sá Maia e-mail: oseiasuesb@gmail.com

Orientador: CAÊ MATOS T. DE ALMEIDA e-mail caemta@yahoo.com.br

Início da orientação: ____/____/____

Data da entrega: ____/____/____.

Caê Matos

Vitória da Conquista – BA 22/11/2021

Digitalizado com CamScanner

UNIFTC

ORIENTAÇÃO DE TRABALHO DE CONCLUSÃO DE CURSO

TERMO DE COMPROMISSO

CARTA DE ACEITE DO ORIENTADOR/CO-ORIENTANDOR

Vitória da Conquista, 22, de novembro, de 2021

Eu, Prof.(a) Caê Matos Teixeira Almeida do colegiado de Direito comprometo-me a orientar os discentes, Bruno Cardoso Lopes, Felipe do Sacramento Batista e Oseias Silva Moreira, regularmente matriculados no curso de Direito na disciplina de TCC II, em seu Trabalho de Conclusão de Curso (TCC) intitulado: Ransomware e lgpd: uma contradição entre fins e meios em caso de extorsão por ransomware.
Declaro pelo presente instrumento, estar ciente das normas que regem o TCC de 2021.2 – UniFTC, divulgado por esta Unidade de Ensino, bem como a disponibilização em formato pdf, em sua versão final, para o Repositório Institucional (RI).

Discentes: Bruno Cardoso Lopes E-mail: brunoc.jus@gmail.com
Discentes: Felipe do Sacramento Batista E-mail: fellipesb.adv@gmail.com
Discentes: Oseias Silva Moreira E-mail: oseiasuesb@gmail.com
Orientador: CAÊ MATOS T. DE ALMEIDA E-mail: caemta@yahoo.com.br

Início da orientação: Data da entrega: 22/11/2021

Para pesquisas de campo encaminhadas ao Comitê de Ética:

Data de aprovação do Comitê de Ética em Pesquisa 06/12/2021
Número do registro: _____

30 de novembro de 2021

Vitória da Conquista/BA

Digitalizado com CamScanner