Instituto de Tecnologia e Sociedade (ITS)

Universidade Estadual do Rio de Janeiro (UERJ)

Direito Penal e Internet

MATHEUS DE MORAIS FALCÃO

Responsabilidade dos Servidores *Cloud Computing* nos Ataques Cibernéticos de Crackers; um Estudo de Caso

Rio de Janeiro

2021

Resumo

Não é nenhuma novidade que vivemos em uma sociedade informática. Computadores quânticos, livre acesso a conteúdo de qualquer parte do globo, consumo de produtos em larga escala e “right on demand”, acesso à informação proveniente das mais diversas emissoras de opinião nos mais diversos países, entre outras diversas atividades que não seríamos capazes de realizar sem essa rede de computadores que trocam constantemente informações. Assim sendo, a internet se consolidou como o instrumento intermediário para as mais diversas atividades cotidianas do ser humano; de ler um livro a se deslocar de um ponto “A” para um ponto “B”.

Contudo, essas informações, dados e elementos referente a pessoa que consome ou usa esse meio intermediário para obter um fim específico, nem sempre estão seguras no ambiente virtual. Muito pelo contrário, não é de hoje que temos conhecimento de ataques cibernéticos à dados pessoais e dados sensíveis de usuários como número de CPF cadastrados em farmácias para se obter descontos, endereço divulgado em aplicativos de transporte, histórico de doenças pelos laudos divulgados por laboratórios de manipulação entre diversos outros elementos.

Sendo assim, resta-se cristalino tal entendimento ao analisar o maior vazamento de dados que ocorreu no Brasil ao qual impactou mais de 223 milhões de brasileiros divulgando dados pessoais e sensíveis como nome, fotografia pessoal, nível de escolaridade, endereço, estado civil, pontuação de crédito e outras informações econômicas, fiscais e previdenciárias. Apesar de ser um acontecimento recente, tais vazamentos de dados não são exclusividade do brasil, nos Estados Unidos, em 2017, foram vazados dados de mais de 147 milhões de consumidores americanos, armazenados pela empresa norte-americana Equifax, atuante na área de gestão de crédito. Dois anos depois, a empresa concordou em pagar ao governo americano 650 milhões de dólares pela falha.

Portanto, é notório que o ambiente virtual não tem uma segurança intrínseca e pode ser utilizado de maneira a práticas delituosas, tendo inclusive feito o nascimento de vários tipos penais ligados a prática delituosa, como o caso do Art. 154-A do Código Penal como apelidado de Lei Carolina Dickman. Esse artigo define o crime de invasão de dispositivo informático e apesar das possíveis críticas tecidas a sua formação, é um instrumento poderoso para a penalização da invasão de crackers nos meios informáticos.

Palavras-chave: Internet. Invasão de Dispositivos. LGPD. Proteção de Dados Sensíveis. Dados e Informações Pessoais. Lei Carolina Dickman. Artigo 145-A do Código Penal. Maior Invasão do Brasil. Invasão de Dispositivos USA. Segurança Virtual. Servidores Nuvem. Cloud Computing.

Abstract

It's nothing new that we live in a computer society. Quantum computers, free access to content from any part of the globe, large-scale consumption of products and "right on demand", access to information from the most diverse opinion stations in the most diverse countries, among other diverse activities that we would not be able to perform without this network of computers constantly exchanging information. Therefore, the internet has consolidated itself as the intermediary instrument for the most diverse daily activities of human beings; from reading a book to moving from point "A" to point "B".

However, this information, data and elements referring to the person who consumes or uses this intermediary means to obtain a specific purpose, are not always safe in the virtual environment. On the contrary, it is not today that we are aware of cyber attacks on personal data and sensitive data of users such as CPF number registered in pharmacies to obtain discounts, address disclosed in transport applications, history of diseases by reports released by laboratories of manipulation among several other elements.

Thus, this understanding remains crystal clear when analyzing the biggest data leak that occurred in Brazil, which impacted more than 223 million Brazilians by disclosing personal and sensitive data such as name, personal photo, education level, address, marital status, score credit and other economic, tax and social security information.

Despite being a recent event, such data leaks are not unique to Brazil, in the United States, in 2017, data from more than 147 million American consumers were leaked, stored by the American company Equifax, which operates in the area of management of credit. Two years later, the company agreed to pay the US government $650 million for the failure.

Therefore, it is clear that the virtual environment does not have an intrinsic security and can be used for criminal practices, having even given rise to several criminal types linked to criminal practice, such as the case of Article 154-A of the Penal Code as nicknamed the Carolina Dickman Law. This article defines the crime of hacking a computer device and, despite the possible criticisms made to its formation, it is a powerful instrument for penalizing the invasion of crackers in computer media.

Keywords: Internet. Device Invasion. LGPD. Sensitive Data Protection. Personal Data and Information. Carolina Dickman Act. Article 145-A of the Penal Code. Largest Invasion of Brazil. Invasion of USA Devices. Virtual Security. Cloud Servers. Cloud Computing.

Sumário

1 Introdução

Inicialmente, o presente artigo tem como objetivo ilustrar os direitos e deveres dos consumidores do serviço nuvem, bem como ônus do serviço prestado pelos servidores de armazenamento na nuvem, usando-se de um caso para tecer comentários e guiar a narrativa das responsabilidades e desdobramentos das esferas consumerista, administrativa e penal. Dessa forma, tenho como meta conscientizar as empresas para a melhor forma de lidar com eventos de incidentes de segurança de maneira aversiva aos adotados no caso em tela.

Desse modo, o presente Inquérito Policial serve como base para o entendimento do melhor modo de agir judicialmente quando algum ataque relacionado a Pessoas Jurídicas e seus dados armazenados na nuvem que acabam impactando tanto informações privilegiadas, quanto economicamente a empresa, inclusive na sua moral para com os seus clientes.

Assim sendo, há de se entender que não existe uma única via de responsabilização quando tratamos de crimes cibernéticos ou LGPD, isso porque como forma tutela Estatal as mais diversas responsabilidades se dão em esferas distintas, como citado anteriormente. Ensejando multas, indenizações ou até prisão preventiva dos que ensejaram o crime.

Para tanto, deve ser entendido os crimes cibernéticos se dão e qual o objetivo no uso desse meio para obter vantagens indevidas, bem como as diferentes imputações penais dos crimes praticados no meio da internet. Ademais, cabe mencionar que apesar da conduta delitiva penalmente ser desempenhada pelo conjunto de pessoas físicas ou pelo invasor, ainda há responsabilização por parte dos servidores na nuvem que deveriam entregar um serviço de qualidade e segurança para seus usuários sejam eles pessoa físicas ou pessoas jurídicas e não o fazem. Contudo, essa responsabilização deve ser feita através do Código do Consumidor.

Por fim, mas não menos importante, quando falamos em Incidente de Segurança e proteção de dados há de pensar diretamente na Lei Geral de Proteção de Dados (LGPD), e o entendimento não está errado. Contudo, para ser possível responsabilizar penalmente a Empresa que sofre um Incidente de Segurança devem ser analisado o seu comportamento perante o incidente. Cabe analisar se foram seguidas as etapas e procedimentos para prevenir e remediar os danos causados, a luz sempre da publicidade dos procedimentos à Pessoa lesada pelo vazamento de dados.

2 Ataque Cibernético aos Servidores AWS – Estudo de Caso[1]

Dessa forma, precisamos a priori entender o caso em tela que exemplifica de maneira nítida quais os impactos de um incidente de segurança e como as Empresas podem mitigar os danos gerados. Assim, o presente caso se resume da seguinte forma; uma Startup relacionada a demandas de tecnologia da informação e automatização de processos jurídicos detinha várias máquinas virtuais de seus sistemas hospedados no servidor nuvem da Empresa AWS, ao qual detinha contrato de prestação de serviços.

Sendo que, em um certo mês identificou, através da fatura do uso dos servidores, que havia uma discrepância gigantesca nos valores de sua fatura. Levando, a após investigação interna descobrir que havia duas máquinas a mais cadastradas e operando em seus servidores na nuvem. Desse modo, somente essas duas máquinas ligadas gastavam mais do que todas as outras 8 (oito) rodando juntas e que, portanto, o gasto de energia e monetário para a utilização das mesmas era de valor estrondoso, completamente discrepante com a atividade de automatização de processos jurídicos desempenhado pela empresa.

Após análise interna e em conjuntura com o Gestor da AWS, fora identificado que as máquinas criadas foram colocadas no sistema simulando o acesso de um dos funcionários da startup e que fora criada a partir de um IP de Oregon nos Estados Unidos. Esse fora o primeiro ataque sofrido e incidente de segurança gerado, uma vez que as máquinas contêm informações de procedimentos e dados dos mais diversos clientes das operações da Startup, o que prejudica diretamente sua imagem com sua carteira de clientes.

No mais, fora identificado que, possivelmente, pelo gasto energético e pelo calibre das máquinas cadastradas, ambas foram utilizadas para minerar criptomoedas se passando por máquinas de um cliente do servidor da nuvem, para camuflar essas máquinas das demais e assim passar por desapercebida. Atitude essa que funcionou durante 1 mês, só vindo a ser notada a partir da exorbitante fatura.

Sendo assim, mesmo após mudança de senhas de usuários pelos colaboradores, no dia seguinte fora identificada nova tentativa de fraude e cadastramento de máquinas, agora com o IP maquiado para o centro de São Paulo. Todas essas comunicações foram feitas entre a AWS e a Startup, ou seja, prestadora de serviço e cliente para que assim fosse identificado como se deu o ataque ou onde estava a falha de segurança do servidor.

Levando em consideração essas informações, podemos perceber como realmente existe uma ideia de riqueza, como foi o petróleo foi para a indústria, com a proteção de dados. Fundamentando essa constatação pela capa da revista The Economist “The world’s most valuable resource”. Com uma simples identificação de clientes de servidores nuvem da Amazon e sabendo a quantidade de máquinas e uso das mesmas foi possível saber quem seria alvo de um ataque cibernético que causou um prejuízo de USD 179.260,66 para os cofres da Startup pelo serviço (indevido) cobrado. Sem contar, claro, o valor minerado em criptomoedas no período de usufruto dos servidores indevidamente.

Ademais, outro fato interessante de ser ressaltado circunda a publicidade dos atos de

[1] Inquétiro Pólicial de Nº 1501834-76.2021.8.26.0050 - 3ª Delegacia de Crimes Cibernéticos (DCCIBER)

contenção do Incidente de Segurança. Explico, quando acontecem as fraudes e invasões de dados que impactaram nos dados pessoais ou dados sensíveis das empresas clientes da Startup; uma política de atitudes deveria ser tomada visando mitigar os riscos desse ataque e prevenir futuros que venham a danificar outros. Somente a primeira atitude segundo os ditames da LGPD foi feita: a troca de senhas de acesso e verificação dos possíveis causadores do incidente.

A segunda etapa após o incidente de segurança é observar as seguintes perguntas quais medidas técnicas a Empresa utiliza para compartilhar os dados, essas técnicas são adotadas ou desempenham o papel de códigos de gaveta? Os sistemas de segurança estão atualizados e funcionando em tempo integral? Existe uma política de atualização desse bloco de questões com uma certa periodicidade?

Para além disso e superada a fase de verificação dos sistemas de defesa e técnicas a fim de coibir um novo ataque ou deixar o sistema mais seguro e sólido, vem a etapa de verificar ou implementar políticas internas e práticas de segurança da informação; ou seja, fazer registro, implementar políticas internas de gestão de incidentes, revisitar o relacionamento com os parceiros para prever como lidar com o incidente e o impacto nos parceiros, entre outras medidas.

Para que, por fim, verificar o impacto do incidente nos dados da empresa ou de seus clientes e assim, medir qual o investimento necessário para reparar esse ônus e prejuízo economicamente e de prestígio, sempre estabelecendo prioridades nas etapas. Vale lembrar que é de suma importância que quando essas etapas forem sendo tomadas a vítima do incidente de segurança, que teve seus dados atingidos, deve ter total e plena visibilidade das atitudes de proteção e mudanças de paradigmas, segundo o princípio da publicidade elencado pela LGPD.

No caso em tela, restou-se petrificado somente a primeira etapa, ao qual a Empresa identificou os dados atingidos e mudança de registros de acessos. Sendo assim, unicamente divulgado para o cliente vítima após insistentes trocas de e-mails perguntando quais medidas estavam sendo tomadas. Ora, vemos, portanto, que a publicidade da reparação do incidente de segurança também não foi respeitada.

3 A Responsabilidade Civil dos “Cloud Computing Sistem”

A cloud computing, ou computação em nuvem é a entrega da computação como um serviço ao invés de um produto, ao qual recursos compartilhados, software e informações são fornecidas, permitindo o acesso através de qualquer computador, tablet ou celular conectado à Internet.

Dessa forma e por causa da sua praticidade, tal serviço passou a ser utilizado por pessoas físicas e jurídicas muito rapidamente, englobando o escopo dos negócios das empresas com o compartilhamento de documentos e pastas entre seus colaboradores entre outros serviços. Além disso, a nuvem permite que esse conteúdo seja editado e salvo. Assim, quando for aberto em outro equipamento estará atualizado. Essa é uma das grandes facilidades que a computação em nuvem proporciona.

Porém, a nuvem está longe de ser um ambiente seguro, como afirmam as empresas do ramo, pois os estudiosos da área de Tecnologia da Informação (TI) ensinam que nenhum ambiente on-line e, por vezes, off-line, está totalmente livre do ataque de hackers e crackers ou até mesmo de defeitos que levam à perda de arquivos.

Nesse contexto, a função do Direito é entender o caráter mutacional da sociedade e adequar os conflitos oriundos dessas mudanças com uma solução que funcione para ambos os lados e para a sociedade. Portanto, adequando ao contexto dos perigos da internet com os consumidores que se utilizam desse meio para exercer suas atividades laborais.

O armazenamento de conteúdos em nuvem vem crescendo no Brasil, segundo dados obtidos pela Growth from Knowledge (GfK), uma empresa alemã especializada, desde 1934, em pesquisa de mercado. Segundo apurado em levantamento recente, os usuários brasileiros consideram essencial o acesso ou armazenamento em nuvem, o que coloca o País em segunda posição, entre vinte e dois países investigados, só perdendo para o México, considerado "líder mundial da nuvem".

Tais dados evidenciam que os brasileiros estão aderindo cada vez mais às Tecnologias da Informação e Comunicação (TIC), e buscam novidades aliadas à praticidade, como a computação em nuvem. Para dar conta dessa demanda crescente existem inúmeros Cloud Computing Providers no mercado nacional e internacional, com destaque para os principais que, segundo Higa[2], são considerados pelos consumidores os melhores provedores. Nessa lista encontram-se o Google Drive, o OneDrive, o Dropbox e a Amazon Web Services, essa última já mencionada no estudo de caso.

Os doutrinadores, como Marcel Leonardi[3], estabelecem uma classificação aos provedores de serviços de Internet. Os Cloud Computing Providers podem ser enquadrados como provedores de hospedagem, haja vista que oferecem espaço na rede para o armazenamento de arquivos, além de possibilitarem que terceiros acessem esses dados, desde que previamente estipulado.

Ademais, esse serviço normalmente é ofertado de forma onerosa, podendo haver remuneração direta ou indireta por parte do consumidor – esta segunda ocorre quando o consumidor tem franqueado o acesso aos serviços em troca da permissão para que seus dados sejam disponibilizados a empresas terceiras, o que o torna alvo de posterior envio de publicidade.

Ocorre que com a advento da Lei Nº 12.965 de 2014, conhecida também como Marco Civil da Internet, os provedores receberam nova denominação, pois tal normativa trouxe em seu texto as expressões "provedor de conexão à internet" e "provedor de aplicações de internet".

O primeiro refere-se aos provedores de acesso ou de conexão à Internet, não havendo grandes dificuldades quanto a essa conclusão. Já o segundo "é um termo que descreve qualquer empresa, organização ou pessoa natural que, de forma profissional ou amadora, forneça um conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à

---

[2] HIGA, Paulo. **Comparativo: os melhores serviços de armazenamento de arquivos na nuvem.** Tecnoblog. 02 fev. 2016. Disponível em: . Acesso em: 7 mar. 2021

[3] LEONARDI, Marcel. **Responsabilidade civil dos provedores de serviços de Internet.** São Paulo: Editora Juarez de Oliveira, 2005.

internet, não importando se os objetivos são econômicos"[4].Disso se extrai que os provedores de hospedagem, e assim os Cloud Computing Providers, nada mais são do que provedores de aplicações de Internet.

Portanto diante de todo mencionado, há de se afirmar que a legislação aplicável ao caso é o Código de Defesa do Consumidor, pois a relação existente entre os provedores de computação em nuvem e os seus clientes é uma relação de consumo, conforme dispõe os artigos 2º e 3º respectivamente a respeito da caracterização de consumidor e fornecedor.

> "**Art. 3°** Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços."

Desse modo, há de se falar em Responsabilização Objetiva na relação de consumo, entendimento esse positivado no cerne do artigo 14 do Código de Defesa do Consumidor. Conforme demonstra o próprio enunciado:

> "**Art. 14.** O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos."

Ainda nessa linha de raciocínio, a Empresa provedora de serviço de armazenamento de arquivos virtuais, oferece além de praticidade ao acesso da informação em qualquer parte do mundo pelo simples fato de ter acesso a internet, também afirma que como uma seguradora de dados na nuvem esses são armazenados de maneira "confiável, escalável e principalmente seguro para a proteção de seus dados".

Nesse sentido, mesmo que não seja mencionado a qualquer momento responsabilidade da Amazon no contrato de prestação de serviço ou nos termos de uso da utilização dos dados pela Empresa ré, afirma o Código Civil:

> "Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito."

> "Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.
>
> Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou

[4] CEROY, Frederico Meinberg. **Os conceitos de provedores do Marco Civil da Internet.** Set. 2014. JusNavigandi. Disponível em: . Acesso em: 10 mar. 2021.

> quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem."

No mais, reitera o entendimento da responsabilidade por parte da AWS o Marco Civil da Internet em especial o artigo 10º e seu parágrafo 4º do mesmo código:

> "Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas."
>
> § 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Em conjuntura com o códice mencionado anteriormente, a Lei Marco Civil da Internet dispõe alguns princípios na utilização de dados e do uso da internet para seus usuários e empresas desse meio tais quais; (Art. 3º, II) Proteção à Privacidade, (Art. 3º, III) Proteção dos Dados Pessoais, (Art. 3º, V) Preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas, bem como (Art. 3º, VI) Responsabilização dos Agentes de Acordo com suas Atividades, nos termos da lei.

No mais, e complementando o entendimento basilar posto, o Marco Civil da internet reforça o dever de indenizar o consumidor lesado, seja ele pessoa física ou jurídica:

> "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I - Inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;"

Por fim, mas não menos importante, cabe uma analogia entre um servidor de armazenamento de dados na nuvem e uma empresa de segurança de dinheiro em cofres de um banco, por exemplo. Ora, se alguém contrata o serviço de um banco para armazenar uma quantia de dinheiro e, assim, protegê-las dos perigos que assolam a sociedade, a mesma coisa acontece quando alguém deposita uma série de informações e dados em servidores na nuvem para assim protege-los de invasores ou de mal-uso por funcionários.

Sendo que, caso haja algum dano a esses dados ou divulgação desses segredos

armazenados, ocorreu uma falha na prestação do serviço contratado. Visto que, segurança é se não um dos principais pilares do objetivo da contratação do serviço. Podemos identificar essa analogia sendo aplicada nos Tribunais Pátrios como o exemplo do julgado de número 0706195-42.2020.8.07.0016[5].

Nesse caso, a magistrada reconheceu a responsabilidade objetiva do banco e julgou parcialmente procedente o pedido autoral para condená-lo a ressarcir à autora a quantia de R$ 29.989,70, a título de danos materiais, e R$ 5 mil, a título de danos morais. Com informações da assessoria de imprensa do TJ-DF.

4 Mas e os "Hackers" que Realizaram o Ataque Cibernético?

Primeiro de tudo, é preciso explicar a origem desses termos e se está sendo usado corretamente. A ideia do Hacker como inimigo da internet remonta um imaginário construído pelas empresas de software ao qual, quando tinham seus sistemas apontados como falhos em algum segmento de sua comunidade de programadores resolveram patentear o uso dos mesmos e extinguir essa cooperação.

Sendo assim, com esse bloqueio da atualização e aprimoramento da segurança desses sistemas, realizado quase que inteiramente pela comunidade de desenvolvedores, no começo dos tempos dos computadores, foi-se criando uma ideia do hacker inimigo. Veja bem, o hacker nada mais é uma pessoa que descobre falhas em sistemas operacionais ou de internet e vende as soluções para as empresas ou a troca de participar do time interno ou por um prêmio em dinheiro pelo aprimoramento. Claro que de maneira amistosa e como troca mercantil.

Desse modo, o significado no dicionário da palavra "Hack" é justamente ressignificar o uso daquele objeto, como acontecia nos primórdios do computador que a cada aprimoramento do sistema a coisa ia sendo ressignificada. Contudo, como já mencionado, nem sempre a palavra foi usada de maneira correta. Assim, a mídia e as corporações de softwares deram a roupagem de hacker para diferentes formas com a cisão da parceria com os desenvolvedores (Hackers); pirateador de conteúdo, navegador de browser, traficante, golpista, terrorista, sempre acompanhado na mídia do pedófilo.

É possível, diante dessa gama de conteúdo, traçar um paralelo com a caça às bruxas e o valor imputados nos hackers com o advento da internet, julgando a atividade "mística", para os leigos, como algo perverso e danoso para a comunidade. Assim, foi-se construindo discursos para fortificar o uso da lei e a vigília dentro nos domínios da internet, para que esses "criminosos" não pudessem atuar.

Em contrapartida desse entendimento, há a figura do "Cracker". Por sua vez, esse desenvolvedor tem como objetivo ferir os sistemas e descobrindo as suas brechas e extorquir as empresas ou usuários do sistema para pagar um valor de resgate do sistema. Por exemplo, um caso famoso de ataque de crackers foi na Empresa Fedex em 2019 ao qual invadiram seu sistema, criptografaram ele todo e ofereceram um valor para entregara contra chave capaz de descriptografá-lo.

---

5 Tribunal de Justiça do Distrito Federal (TJDF), 4º Juizado Especial Cível de Brasília, número: 0706195-42.2020.8.07.0016, Relatora: Oriana Piske

Essa é a principal diferença de ambas as atuações e está justamente dividida quanto ao dolo do agente, de um lado o agente que tende como objetivo aprimorar a segurança e consequentemente o sistema desejado e por outro lado alguém que versa por danificar a empresa e lucrar em cima disso. Cabe aqui fazer um adendo, pois existe crime previsto para essa prática delitiva de extorsão na internet chamada de criptoviral e consta no Artigo 158 do Código Penal.

A recomendação nesses casos é de não pagar a recompensa pela descriptografia, pois muitas vezes não existe uma. Os criminosos desconfiguram o sistema, mas não fazem uma chave para quebrar essa criptografia, por motivo de ser muito trabalhoso e difícil e visto que o objetivo deles já fora consumado com a invasão, tem o pensamento comum de não realizar o procedimento. Portanto o indicado é acionar as autoridades policiais especializadas em crimes cibernéticos o mais rápido possível para solucionar a demanda e começar as investigações.

Desse modo, conseguimos identificar outra diferença entre as duas condutas, na atividade de extorsão para pagamento de prêmio o crime de extorsão já existe no Código Penal e pode ser aplicado na realidade do mundo concreto. Nesse caso ele somente está na roupagem da internet, ou seja, não é um crime cibernético, mas um crime praticado pelo meio digital.

Notório que no caso em tela narrado, não há atividade de hackers, mas de crackers que invadiram os sistemas na nuvem da Empresa e simularam a abertura de uma nova máquina através de um suposto "maqueamento" de usuário no intuito de minerar criptomoedas.

Por outro lado, conseguimos identificar que nesse caso se trata de um crime cibernético ao qual sem o meio informático não há de se falar no mesmo fato típico e antijurídico cuja narrado no artigo 154-A do Código Penal. Insta salientar que tal dispositivo fora adicionado ao códice através da Convenção de Budapeste, tratado internacional esse que dispusera sobre Crimes Cibernéticos e como coibi-los.

> **"Art. 154-A.** Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
>
> **§ 3º.** Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: (Incluído pela Lei nº 12.737, de 2012) Vigência Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave."

Portanto, analisando o fato típico do artigo 154-A é possível tecer alguns comentários aplicáveis no caso em tela. Primeiro de tudo que como no caso foi simulado o acesso de um dos usuários do sistema na nuvem pode ser aplicado a tipificação, pois somente se trata de invasão em hardware ou acesso pessoal o disposto penal, apesar do cristalino entendimento na convenção de Budapeste englobar a invasão de softwares também.

Cabe identificar que no trecho “com o fim de obter, adulterar ou destruir dados ou informações” demonstra a real diferença na imputação criminal no tipo penal, pois não são os hackers que realizarão essa ação, mas então somente os crackers. E por fim, há ainda uma qualificadora no tocante a natureza da invasão, caso ela obtiver comunicações privilegiadas, segredos industriais ou informações sigilosas.

Ora, a qualificadora se adequa como uma luva no caso narrado, pois além dos invasores saberem o tipo de maquinário utilizado pela Empresa e as funções realizadas com cada máquina registrada no servidor, ainda tem acesso a todos os dados que essas máquinas são alimentadas com informações dos clientes e operações vigentes.

Diante de todo o exposto, a responsabilização penal pelos crimes do artigo 154-A, §3º com o aumento de pena do §2º por ter gerado um gritante prejuízo econômico para a empresa lesada é translúcido e de vital importância.

5 Responsabilidade Administrativa dos Servidores Cloud

Sendo assim, cabe indicar que, não obstante as outras responsabilizações, o ataque ao sistema dos servidores na nuvem gerou uma responsabilização segundo a Lei Geral de Proteção de Dados como irei demonstrar. Ora, no caso em tela existe uma empresa que guarda suas informações de operações e máquinas tais quais, computadores e hardwares para que suas operações funcionem em servidores na nuvem. O que houve foi uma invasão nesse servidor, que continuou funcionando com todos os dados e informações das operações com os clientes, ao passo que, concomitantemente foram geradas duas máquinas fantasmas pelos criminosos com o intuito de minerar criptomoedas.

Cabe salientar que mesmo que os criminosos, aparentemente, não tenham atuado nas máquinas operantes nas mais diversas operações dos clientes, eles tiveram acesso a todas essas informações ao invadir o servidor na nuvem. Assim, dados sensíveis de operações da empresa com clientes, informações das máquinas e configurações do core business da empresa entre outros diversos dados utilizados para venda de informação.

Além disso, há de se falar em sanção administrativa para o desrespeito à regra da publicidade do incidente de segurança para a vítima que sofreu o dano, coisa que em nenhum momento pode ser observada por parte da AWS no presente caso. A única informação prestada fora a de troca das senhas e usuários, mas todas as outras medidas para prevenir e remediar o dano não passaram e nem muito menos foram informadas para a empresa vítima o que ocasiona sanções administrativas com caráter de punição para educar.

Ademais, resta destacar que em seu artigo 44, a LGPD, deixa claro que o tratamento de dados pessoais será irregular quando não fornecer a segurança que o titular dele pode esperar, o que reforça tudo que fora dito ao longo desse artigo. Portanto, um vazamento de dados pode levar à aplicação de sanções administrativas previstas na lei, muito embora que elas só poderão ser aplicadas a partir de agosto de 2021, pois ainda não foram implementadas diretrizes que guiem as autoridades em matéria de LGPD para sancionar.

Cabe salientar que as sanções previstas na LGPD serão aplicadas conforme o devido

processo legal administrativo, com o respeito ao contraditório, ampla defesa e direito ao recurso. Sempre se pautando nos parâmetros e critérios previstos em lei, tais como a cooperação do infrator, a pronta adoção de medidas corretivas e a implementação de mecanismos internos para o tratamento adequado dos dados.

Portanto esse entendimento de dever de sanção administrativa à empresa que desrespeita algum(ns) parâmetros da LGPD tem como objetivo além de impor a força legislativa e educar para que toda a comunidade se adeque as normas impostas, mostrar que um incidente de segurança, por exemplo, gera impactos estrondosos para a vítima tais quais: (i) Perdas financeiras por conta de negócios cancelados, fuga de investidores e vazamento de informações sensíveis à empresa; (ii) Quebra de confiança na relação com o consumidor e com os titulares de dados em geral e (iii) Danos de reputação e imagem.

Dessa forma é notório que a melhor estratégia para as empresas é adotar uma postura preventiva e de adoção das medidas de segurança a fim de evitar qualquer incidente possível. Nesse mesmo raciocínio as possíveis sanções aplicadas podem ser dá mais branda para a mais severa: (i) Advertência, com prazo para corrigir as infrações; (ii) Multa simples de até 2% do faturamento da empresa no ano anterior, até o limite de R$50 milhões por infração; (iii) Multa diária de até 2% do faturamento da empresa no ano anterior, até um limite de R$50 milhões por infração; (iv) Tornar pública a infração cometida; (v) Bloqueio dos dados pessoais relacionados à infração; (vi) Eliminação dos dados pessoais relacionados à infração; (vii) Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período; (viii) Suspensão da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período e (ix) Proibição parcial ou total das atividades relacionadas a tratamento de dados.

Isto posto, resta-se claro que a empresa AWS tem responsabilidade administrativa a luz dos mandamentos da LGPD diante do todo exposto. Ademais, outra conclusão que podemos obter após analisar as nove possíveis sanções aplicáveis é a máxima de que a melhor alternativa para as empresas é o devido respeito as normas da lei geral de proteção de dados assim como o devido respeito aos procedimentos adotados após o incidente de segurança para minimizar as sanções sofridas.

6 Conclusão

Dessa forma, com esse artigo meu objetivo foi em primeiro momento analisar o caso descrito do incidente de segurança que ocorreu nos servidores da Amazon e em especial com a invasão de crackers às máquinas de uma empresa cuja operação é automatizar processos jurídicos. Isso posto, resolvi tecer alguns comentários acerca das possíveis responsabilidades civis, penais e administrativas dos responsáveis na medida de suas culpas.

Diante de tal análise há de se falar que a responsabilidade penal somente pode ser imputada a figura da ou das pessoas que praticaram o crime do art. 154-A do Código Penal. Isso porque mesmo que seja uma invasão a software se deu através de simulação de chaves de acesso, além disso, não há outro crime possível de dolo e/ou culpa para a Empresa que gere os servidores na nuvem.

Contudo, a alternativa de penalização para os Cloud Computer Sistem são duas; uma relacionado ao Código de Defesa do Consumidor em conjuntura com o Marco Civil da Internet e outra administrativa conforme os ditames da LGPD. Logo, em matéria consumerista, o serviço prestado apresenta falhas, pois se diz promovedor de segurança ao armazenar os arquivos desejados como numa analogia com um banco que "guarda" seu dinheiro e finanças, possuindo câmeras de segurança, guardas armados, fortificação, entre outras medidas de segurança.

Assim, caso o banco sofra algum ataque passível de penetração em seus aposentos e assim prejudicando quem confiou no serviço prestado, deverá indenizar a vítima a título de danos morais e materiais no que fora perdido. O mesmo, portanto, ocorre com os servidores na nuvem, oferecendo segurança no armazenamento de dados, deveria, portanto, ter mecanismos para verificar os usuários que entram no sistema e outros mecanismos de segurança capazes de dirimir os possíveis ataques e minimizar seus danos.

Dito isso, chegamos no último segmento do artigo, no caso em tela, mesmo não tendo os mecanismos de segurança para prevenir o incidente de segurança, a AWS deixou de praticar as diretrizes de tratamento dos dados bem como a publicidade de seus atos para a empresa vítima do ataque. O que, por si só, caracteriza uma grave falha e desrespeito à Lei Geral de Proteção de Dados, ensejando punição administrativa após o devido processo legal administrativamente.

Portanto, tentei por meio desse artigo ilustrar, na prática os possíveis caminhos de responsabilização dos entes usando as leis e matrizes jurídicas nacionais com o objetivo de mitigação dos futuros erros e justiça para o polo mais fraco da relação que sempre é e sempre será a vítima.

7 Referência Bibliográfica

1. CASTELLS, Manuel. (2006), **A Era da Informação: Economia, Sociedade e Cultura**. vol. 1, A Sociedade em Rede. 9 ed. São Paulo: Paz e Terra.
2. CEROY, Frederico Meinberg. **Os conceitos de provedores do Marco Civil da Internet**. Set. 2014. JusNavigandi. Disponível em: . Acesso em: 10 mar. 2021.
3. GRAGLIA, Marcelo Augusto Vieira; LAZZARESCHI, Noêmia. **A Indústria 4.0 e o Futuro do Trabalho:: Tensões e Perspectivas. Revista Brasileira de Sociologia**, [S. l.], v. 6, n. 14, p. 110 - 146, 20 dez. 2018.
4. HIGA, Paulo. **Comparativo: os melhores serviços de armazenamento de arquivos na nuvem.** Tecnoblog. 02 fev. 2016. Disponível em: . Acesso em: 7 mar. 2021
5. MONTEIRO, Renato Leite; GOMES, Maria Cecília Oliveira; NOVAES, Adriane Loureiro. et al. **Lei Geral de Proteção de Dados e GDPR: Histórico, análise e impactos**;
6. LEONARDI, Marcel. **Responsabilidade civil dos provedores de serviços de Internet.** São Paulo: Editora Juarez de Oliveira, 2005.
7. MULHOLLAND, Caitlin (org.). **LGPD e o novo marco normativo no Brasil**;
8. PRESIDÊNCIA DA REPÚBLICA, CASA CIVIL, SUBCHEFIA PARA ASSUNTOS JURÍDICOS. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940.** Código Penal. [S. l.], 7

dez. 1940.

9. PRESIDÊNCIA DA REPÚBLICA, CASA CIVIL, SUBCHEFIA PARA ASSUNTOS JURÍDICOS. **Decreto-Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências - Código de Defesa do Consumidor. [S. l.], 11 set. 1990.

10. PRESIDÊNCIA DA REPÚBLICA, CASA CIVIL, SUBCHEFIA PARA ASSUNTOS JURÍDICOS**. Lei nº 10.406, de 10 de janeiro de 2002.** Institui o Código Civil. [S. l.], 10 jan. 2002.

11. PRESIDÊNCIA DA REPÚBLICA, CASA CIVIL, SUBCHEFIA PARA ASSUNTOS JURÍDICOS. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil - Marco Civil da Internet. [S. l.], 23 abr. 2014.

12. SANTOS, Juarez Cirino dos. **Política criminal: realidade e ilusões do discurso penal.** Discursos Sediciosos, Rio de Janeiro, v. 1, p.53-57, 2002;

13. SILVA, Rosane Leal da; FAVERA, Rafaela Bolson Dalla; OLMOS, Olívia Martins de Quadros. **A responsabilidade civil dos principais cloud computing providers em razão da perda de arquivos.** Revista da Faculdade de Direito UFPR, Curitiba, PR, Brasil, v. 63, n. 2, p. 89-113, ago. 2018. ISSN 2236-7284. Disponível em: . Acesso em: 07 março. 2021. DOI: http://dx.doi.org/10.5380/rfdufpr.v63i2.58628.

14. SILVEIRA, Renato de Mello J. **Bitcoin e suas fronteiras penais:: em busca do marco penal das criptomoedas**. 2. ed. rev. Belo Horizonte: D'Plácido, 2018. 49 - 79 p;

15. SYDOW, Spencer T. **Crimes Informáticos e suas vítimas: de acordo com a Lei n. 12.965, de 2014 - Marco Civil da Internet.** 2. ed. São Paulo: Saraiva, 2015;

16. TEFFÉ, Chiara Spadaccini de. **A saúde na sociedade da vigilância: como proteger os dados sensíveis?**. Migalhas, [s. l.], p. 1 - 4, 14 abr. 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-vulnerabilidade/324485/a-saude-na-sociedade-da-vigilancia-como-proteger-os-dados-sensiveis. Acesso em: 23 jun. 2021.

17. **THE WORLD'S MOST VALUABLE RESOURCE IS NO LONGER OIL**, BUT DATA. Nova Iorque: The Economist, 2017- . Semestral.

18. Tribunal de Justiça do Distrito Federal (TJDF), 4º Juizado Especial Cível de Brasília, Número: 0706195-42.2020.8.07.0016, Relatora: Oriana Piske

19. VEGH, Sandor. **Hacking for democracy: a study of the internet as a political force and its representation in the mainstream media.** 2003. Tese (Doutorado em Estudos Americanos) – Universidade de Maryland. p. 151-167; p. 207-228;

20. VIANNNA, Túlio Lima. **A ideologia da Propriedade Intelectual: a inconsistência da tutela penal dos direitos patrimoniais de autor.** Porto Alegre: Ajuris, 2005. 243 p. v. 99;

21. ZAFARRONI, Raul**. O Inimigo do Direito Penal**. 3. ed. atual. Instituto Carioca de Criminologia: Revan, 1940. 11 a 27 p;

22. ZAFFARONI, Eugenio Raúl. **Em busca das penas perdidas**. Rio de Janeiro: Revan, 1991 – parte I, p. 11-45;