LAVAGEM DE DINHEIRO E ATAQUE RANSOMWARE – A NOVA FRONTEIRA

MONEY LAUNDERING AND RANSOMWARE ATTACK - THE NEW FRONTIER

CLAUDIA DA COSTA BONARD DE CARVALHO[1]

RESUMO: O presente artigo trata da possibilidade de Lavagem de Dinheiro relacionada ao ataque cibernético *ransomware*, no qual é exigido o pagamento de criptomoedas para a liberação de acesso a dados bloqueados, o que tem sido difundido por indústria de negociadores profissionais, em desacordo à orientação da polícia de todos os países e já está sendo coibido pelo gabinete de Combate de Crimes Financeiros do Tesouro norte-americano, tendo em vista que poderá ser simulado por empresas, como forma de obter-se autorização corporativa para movimentar quantias de origem ilícita, através de suposta medida de viabilização de retorno das atividades, devido a provável existência de interesses escusos de membros da alta direção na operação, viabilizados pelo *cybercrime*.

Palavras-Chave: lavagem, dinheiro, ransomware, resgate, criptomoedas, cybercrime

Abstract: This article deals with the possibility of Money Laundering related to the cyber attack ransomware, in which the payment of cryptocurrencies is required to release access to blocked data, which has been disseminated by the industry of professional negotiators, in disagreement with the police guidance from all countries and is already being restrained by the US Treasury's Financial Crimes Fighting office, given that it can be simulated by companies, as a way to obtain corporate authorization to move amounts of illicit origin, through supposed measure to enable the return of activities, due to the probable existence of vested interests of members of senior management in the operation, made possible by cybercrime

Keywords: laundering, money, ransomware, rescue, cryptocurrencies, cybercrime

---

[1] A autora é advogada criminal especializada em Compliance Digital, Cybersecurity e Legal Advisor em Cybercrime, graduada pela UERJ e Pós - Graduada em Direito Penal e Processo Penal pela Universidade Estácio de Sá.

1-INTRODUÇÃO

Empresas do mundo todo tem sido alvo da ação de cybercriminosos, causando graves transtornos operacionais, prejuízos financeiros e perda reputacional, pelo que, as estatísticas de ataque cibernético apenas aumentam a cada ano.

Pesquisa recente da empresa KROLL[2] aponta que, somente em 2019, um dos riscos que mais afetaram as empresas, o qual foi considerado um dos mais relevantes, é a subtração de dados, os quais, na atual sociedade da informação, valem muito dinheiro e são o centro da atividade criminosa na internet.

Neste contexto de ataques cibernéticos, um dos mais complexos e difundidos pela internet, é o ataque *ransomware*, o qual é praticado por classe de cybercriminosos ora denominados econômicos, os quais atingem especialmente as empresas com extorsões digitais (conduta assemelhada ao tipo penal do artigo 158 do Código Penal - **Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa**), ameaçando suas vítimas de perda de dados, caso não se efetue pagamento de seu resgate em criptomoedas.

Frise-se que, o pagamento de resgate de *ransomware* é medida totalmente desestimulada pelas autoridades policiais mundiais, tendo em vista a ausência de garantia de recuperação de dados e pelo financiamento do *cybercrime.*

No entanto, o pagamento de um resgate, aparentemente feito como forma de retomada de acesso a dados bloqueados, poderá disfarçar o cometimento de crimes financeiros, tendo em vista o surgimento de um mercado de empresas de negociadores de resgate, o que despertou a desconfiança do gabinete de Combate a Crimes Financeiros do Tesouro norte-americano[3].

Ora, a lavagem de dinheiro por criptomoedas já é uma realidade, pelo que, os referidos pagamentos de resgate por ataque cibernético *ransomware* podem facilitar ainda mais a sua ocorrência, sob outras circunstâncias.

Diante disso, existe a possibilidade de simulações de situação de ataque *ransomware*, somente para justificar movimentação de quantias ilícitas por empresas em favor de terceiros, o que pode ser feito para encobrir interesses de executivos que praticam atividades criminosas, como lavagem de dinheiro.

---

[2]KROLL, Onde eles estão?**,** Revista Digital Lec ano 8, nº 28, abril/2020

[3]PAGAMENTO DE RESGATE EM CRIPTOMOEDAS. Disponível em: <https://www.uol.com.br/tilt/noticias/reuters/2020/10/01/tesouro-dos-eua-diz-que-empresas-podem-ser-punidas-por-pagarem-resgate-para-hackers.htm>. Acesso em 15.10.2020.

2-CYBERCRIME E ATAQUE RANSOMWARE

Conforme mencionado anteriormente, a informação e o seu acesso passaram a ser ferramentas preciosas para a moderna criminalidade. Neste sentido, LLINARES (2019, p.27) destaca o valor dos dados para o cybercrime

> cuando el protagonismo lo tuvieron las terminales informáticas y la información personal que ellas podían contener, aparecieron nuevas formas de afectar a la intimidad de las personas; cuando dichas terminales y la información en ellas contenida comenzaron a tener valor económico y a servir para la realización de transacciones económicas, surgieron las distintas formas de criminalidad económica relacionadas con los ordenadores y muy especialmente el fraude informático que, a su vez, evolucionó hacia el scam, el phishing y el pharming cuando apareció Internet.

Assim sendo, os dados são o combustível do *cybercrime*, que agora passa a chantagear empresas para obter vantagens financeiras, através de ataque *ransomware*, que caracteriza o inimigo nº 1 das empresas (SCHWARTZ, 2020)**,** por se tratar de um dos incidentes de segurança mais perigosos na atividade corporativa.

O *ransomware*[4] é um tipo de *malware* (software causador de danos) criado para bloquear dados de sistemas, o qual, geralmente, invade redes corporativas por e-mails de *phishing* (técnica de *cybercrime* para obtenção de dados), que, ao serem abertos desavisadamente, provocam a instalação do programa indesejado.

Muitas vezes, esse email-*phishing* usa a técnica *typosquatting*[5] (cópia de URL de sites anexados à mensagem) para simular páginas de fornecedores ou prestadores de serviços, que devam ser acessadas para faturamento ou atualização de cadastros, por exemplo, as quais apresentam logos de empresas com cores diferentes ou erros de português nas suas informações, o que passa despercebido pelo leitor desatento, de forma a enganar o colaborador.

Após instalado, o *ransomware* criptografa dados de sistemas e envia uma mensagem de bloqueio de tela por ataque cibernético, solicitando o pagamento de resgate, sob pena de perdimento das informações bloqueadas.

Existem muitos tipos de *ransomware* já detectados, sendo que, tais bloqueios de informações podem causar grandes prejuízos aos ativos das empresas, conforme a capacidade de resposta de cada uma aos incidentes de segurança informação, cujas diretrizes para gestão de riscos cibernéticos como este são dadas pela norma ISO 27005 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2011).

---

[4]RANSONWARE. Disponível em :https://www.kaspersky.com.br/resource-center/definitions/what-is-ransomware. Acesso em 15.10.2020.

[5]TYPOSQUATTING. Disponível em: <https://pris.com.br/blog/cybersquatting-e-typosquatting-pirataria-no-meio-digital/>. Acesso em 15.10.2020.

Frise-se que, em tempos de vigência da Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/18), as extorsões digitais já são calculadas conforme os valores da multas previstas neste diploma legal, de forma que os cybercriminosos ainda ameaçam divulgar o vazamento de dados pessoais dos sistemas da empresa, caso o referido valor não seja pago pela vítima, o que configura dupla extorsão.

Neste sentido, o pagamento de resgate *ransomware* tornou-se uma infeliz solução para muitas empresas que não investiram em uma estrutura de segurança da informação que possa prevenir um ataque cibernético e acabaram sucumbindo à referida chantagem, por receio de terem seu vazamento de dados exposto, prejudicando, desta forma, sua reputação no mercado.

Cumpre destacar ainda que, somente no Brasil, os ataques *ransomware* contra empresas cresceram de forma espantosa nos últimos anos, sendo considerado, atualmente, o país mais atingido na América Latina pelo *malware*, de acordo com pesquisa desenvolvida pela empresa KASPERSKY[6].

3- A POLÊMICA DELIBERAÇÃO DO TESOURO DOS EUA SOBRE PAGAMENTO DE RESGATE RANSOMWARE

O cenário mundial de crescentes ataques *ransomware* e de falta de medidas preventivas para proteção de sistemas corporativos criou um mercado de profissionais negociadores de resgate, os quais visam ganhar tempo e diminuir as consequências operacionais e financeiras da extorsão para as empresas atingidas.

Ocorre que, nos EUA esse novo serviço começou a despertar a atenção das autoridades de combate ao crime financeiro, pois tal medida seria um incentivo ao *cybercrime* e precisaria ser combatida pelo governo americano.

Diante disso, tais negociações intermediadas por empresas passarão a ser proibidas, conforme deliberado pelo Gabinete de Controle de Ativos Estrangeiros e Combate a Crimes Financeiros do Tesouro dos EUA, devendo ser feitos por supervisão judicial, sendo que, qualquer empresa que deseje atuar dessa forma deverá ainda registrar-se como instituição financeira, tendo em vista que o pagamento do resgate também é feito através do negociador.

Verifica-se, então, que a grande preocupação que existe por trás da referida medida é constatar-se que poderiam ocorrer simulações de ataques cibernéticos, para facilitação de práticas de crimes financeiros, pois as quantias seriam movimentadas por intermediação de terceiros para os cybercriminosos, em situação bastante semelhante à posição dos doleiros que atuam nos casos de lavagem de dinheiro.

---

[6]KASPERSKY. Disponível em: <https://canaltech.com.br/seguranca/brasil-e-o-pais-mais-atingido-por-ataques-de-ransomware-na-america-latina-173018/>.Acesso em 15.10.2020.

No caso, os dirigentes de empresas que pretendam pagar os resgates de *ransomware*, através de negociadores, caso não atendam as referidas diretrizes governamentais, poderão se ver agora na posição de réus e não de vítimas de extorsão.

4-LAVAGEM DE DINHEIRO E SEUS CONTORNOS MAIS TRADICIONAIS

De acordo com a decisão do órgão governamental norte americano acima mencionado, o principal objetivo é combater fraudes financeiras, sendo uma das mais graves a lavagem de dinheiro

A lavagem de dinheiro no Brasil é definida na Lei 9.613/98, que prevê a sua forma mais básica em seu artigo 1º:

> Art. 1º Ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal
>
> Pena: reclusão, de 3 (três) a 10 (dez) anos, e multa.

BADARÓ e BOTTINI (2017, p. 29) definem o crime de lavagem de dinheiro como qualquer ato de esconder a origem ilícita de algum recurso financeiro, para sua reinserção posterior no mercado

> Lavagem de dinheiro é o ato ou consequência de atos praticados para mascarar a natureza, origem, localização, disposição, movimentação ou propriedade de bens, valores e direitos de origem delitiva ou contravencional, com o escopo último de reinseri-los na economia formal com aparência de licitude.

Cabe destacar que, a lavagem de dinheiro será realizada mediante a prática de diferentes atos, descritos em várias etapas, as quais poderão ter a participação de diferentes agentes. SANTOS (2018, p.100) descreve cada uma destas etapas

> A prática de lavagem de dinheiro pode ser observada em três diferentes fases. Uma primeira fase de ocultação ou colocação, denominada placement. Uma segunda fase de dissimulação, chamada layering. E uma terceira fase de integração, a integration ou recycling. Para que o crime seja consumado, não é preciso que se realizem todas as três etapas (Baltazar Junior, 2011, p. 775), as quais podem existir de maneira independente, simultânea ou superposta (De Carli, 2008, p. 118).

Não bastasse isso, a lavagem de dinheiro ainda envolve diversas técnicas, que asseguram a movimentação de quantias de origem ilícita, as quais podem, por exemplo, ser pulverizadas em várias contas bancárias no país ou em paraísos financeiros offshore, o que foi feito para muitos executivos de empresas por doleiros envolvidos na Operação Lava-Jato.

Evidente ainda que tais práticas são bastante disfarçadas nas empresas, podendo estar embutidas no âmbito de muitas operações da sua própria rotina, como pagamentos para fornecedores fictícios, movimentação de quantias sem motivo entre filiais de uma holding e etc.

Vale dizer ainda que, a simples atuação de uma pessoa num determinado momento do *iter criminis* do delito de lavagem de dinheiro, sem que pudesse ter conhecimento ou suspeitar do objetivo de branqueio de ativos por outrem, não poderia acarretar a sua imediata responsabilização. CORDERO (1997, p.268) adverte, com precisão, sobre os riscos ora descritos

> Si se admite la sanción de tales comportamientos en el ámbito del blanqueo de capitales, van a ser punibles acciones tales como la del taxista que transporta a un traficante de drogas y recibe como pago dinero de origen delictivo, la del conductor de autobús que le vende un billete, la de quien utiliza la piscina de un narcotraficante, la del panadero que le vende pan, la del médico que recibe sus honorarios del narcotraficante, etc. (21) Incluso van a quedar abarcados negocios de bagatela, de escasa cuantía, en la misma medida que el blanqueo de miles de millones mediante transferencias financieras internacionales (22). Pero no sólo esto, sino que la recepción de dinero de origen delictivo como pago por la prestación de servicios de carácter profesional a los autores de un delito previo, dirigidos a la asesoría jurídica, financiera, etc., van a ser subsumibles también en el tipo del delito de blanqueo (23). Este problema ha sido ampliamente analizado por la doctrina en referencia a los empleados de entidades financieras. El empleado de banca que cumple las órdenes que le da un cliente que pretende blanquear su dinero puede ser impune si desarrolla su actividad con desconocimiento de su origen delictivo y sin infringir las obligaciones que le impone la ley. Ahora bien, si sospecha del carácter delictivo de los bienes, tiene un conocimiento casual de su origen o actúa por imprudencia grave, la misma acción del empleado de banca sería calificada como blanqueo de capitales. Es exclusivamente este conocimiento o desconocimiento imprudente el que convierte al empleado de banca de trabajador que desarrolla su actividad normal impune, en delincuente por razón del delito de blanqueo de capitales

Insta salientar que, este aspecto da possível suspeita de prática de lavagem de dinheiro será especialmente importante nas tomadas de decisão sobre pagamento de resgate em ataque ransomware, senão vejamos:

5- LAVAGEM DE DINHEIRO POR CRIPTOMOEDAS

Atualmente, a lavagem de dinheiro não se limita a movimentar quantias em moeda corrente, mas também por meio de criptomoedas, como *Bitcoin*, *Ethereum* e demais similares que já circulam no mercado, as quais possuem a

vantagem de facilitar o anonimato de seus negociantes, pela mera utilização de chaves criptografadas.

Além disso, o fato do mercado das criptomoedas não depender de regulação de sistema bancário central, o qual monitora operações suspeitas de clientes, mediante a adoção de normas de *Compliance* bancário (Regras da Basiléia), favorece extremamente a lavagem de dinheiro, pois não há qualquer controle regular de identificação de negociadores, apenas a realização de simples cadastros de usuários de serviços em plataformas digitais (*exchanges*) de câmbio de criptomoedas.

Diante disso, o Banco Central já começou a fiscalizar indiretamente tais operações, exigindo agora que as movimentações em criptomoedas de clientes, a partir de determinado valor, sejam comunicadas pelas *exchanges* ao referido órgão, de acordo com a Instrução Normativa nº 1888/2019

> Art. 6º Fica obrigada à prestação das informações a que se refere o art. 1º:
>
> I – a exchange de criptoativos domiciliada para fins tributários no Brasil;
>
> II – a pessoa física ou jurídica residente ou domiciliada no Brasil quando: a) as operações forem realizadas em exchange domiciliada no exterior; ou
>
> b) as operações não forem realizadas em exchange.
>
> § 1º No caso previsto no inciso II do caput, as informações deverão ser prestadas sempre que o valor mensal das operações, isolado ou conjuntamente, ultrapassar R$ 30.000,00 (trinta mil reais).
>
> § 2º A obrigatoriedade de prestar informações aplica-se à pessoa física ou jurídica que realizar quaisquer das operações com criptoativos relacionadas a seguir:
>
> I – compra e venda;
>
> II – permuta;
>
> III – doação;
>
> IV – transferência de criptoativo para a exchange;
>
> V – retirada de criptoativo da exchange;
>
> VI – cessão temporária (aluguel);
>
> VII – dação em pagamento;
>
> VIII – emissão; e
>
> IX – outras operações que impliquem em transferência de criptoativos.

A existência de monitoramento de valor destas operações é especialmente importante, na medida em que, na circulação deste ativo, em grandes quantidades periódicas ou de forma pulverizada, podem também estar encobertas práticas de lavagem de dinheiro.

Cabe destacar que, já existem técnicas de ocultação de valores provenientes de ilícito que envolvem a "mistura" de moedas de procedência lícita, com outras de origem criminosa, a denominada *Coin Mix,* que foi criada com o intuito de preservar a identidade dos negociadores, mas acabou gerando o risco de lavagem de dinheiro. ESTELITTA (2020, p.5) esclarece como funciona a referida técnica

> Cada usuário remete uma quantidade de moedas virtuais para o mixer e designa um ou mais endereços (geralmente novos) nos quais quer receber a mesma quantia, descontado o preço cobrado pelo serviço de mescla.As moedas, para falar de modo metafórico, são jogadas em uma "piscina" com as moedas de outros usuários, misturadas e, então,remetidas para os endereços designados pelo usuário.A remessa pode, ainda, ser fracionada em diversas pequenas transações, 8 usando diversos provedores de mixing em operações sucessivas. Pesquisas mostram que esses serviços têm o potencial de tornar impossível o rastreamento das moedas, além de implicarem riscos aos próprios usuários, como o de furto ou mesmo de desvio ou perda dos valores pelo encerramento ou bloqueio do serviço (GRZYWOTZ, 2019, p. 106-107)

Ora, não é à toa que o pagamento de resgate em criptomoedas é essencial no ataque ransomware, justamente pela dificuldade de rastreamento destes ativos pelas autoridades policiais e pela possibilidade de serem negociados, posteriormente, em uma *exchange* (corretora de criptomoedas), utilizando-se das referidas técnicas de ocultação de sua origem, o que caracteriza a forma mais conhecida de lavagem de dinheiro eletrônica.

6- SIMULAÇÃO DE ATAQUE CIBERNÉTICO E LAVAGEM DE DINHEIRO

No entanto, apesar do conhecido cenário de branqueamento de criptoativos, surgem agora novas possibilidades de lavagem de dinheiro por criptomoedas, em um contexto de ataque *ransomware* sobre as empresas.

Com isso, em situações de incidente de segurança *ransomware*, a governança de determinada empresa poderá entender que a única forma de resolver a questão é aceitar pagar o resgate e conseguir seus dados de volta, entregando as criptomoedas ao cybercriminoso, mediante atuação de um negociador. No entanto, esta decisão pode ser questionada.

Indaga-se: esse pagamento era realmente necessário? Tal colocação pode ser questionada, de acordo com a atividade da empresa vítima e o grau de risco aos ativos que ela visa preservar, diante do referido ataque cibernético.

Com isso, exemplificativamente, um ataque cibernético em um hospital privado colocaria em risco ativos cuja perda seria extremamente danosa, como os resultados de exames de pacientes, falhas de funcionamento de equipamentos e até mesmo dificuldades para atendimento no local.

Já há notícia, inclusive, de um ataque *ransomware* a hospital privado brasileiro[7], sendo que, felizmente, o seu sistema estava minimamente preparado para responder a incidentes de segurança da informação, bem como não houve dano ao seu funcionamento e nem ao tratamento dos pacientes.

No entanto, na Alemanha[8], uma pessoa foi vítima de um ataque *ransomware,* não podendo ser atendida em estado grave num hospital, cujo sistema caiu, por conta daquele tipo de ataque cibernético, causando a morte da paciente.

Logo, há que se verificar o que está em jogo e se há real necessidade de pagamento de valores. Se fosse o caso desse hospital, que estava evidentemente despreparado, talvez fosse aceitável o referido pagamento, como caso de estado de necessidade, por exemplo, para salvar o bem jurídico-vida dos pacientes internados, sacrificando-se as finanças da pessoa jurídica.

Por outro lado, se estivéssemos diante de caso de atividade diversa, tratando-se de empresa de grande porte, com configurações razoáveis de segurança, o pagamento de resgate em criptomoeda no ataque ransomware seria razoável? Muitas empresas concordam com esta chantagem apenas por receio de mancha reputacional e de desvalorização de suas ações no mercado.

Caso entenda-se o pagamento de resgate como algo necessário: quais os riscos envolvidos nesta atitude? Será que o ataque cibernético poderia ter sido encomendado, como os falsos sequestros de pessoas (aquelas ligações imitando vozes de filhos para assustar idosos e pedir dinheiro)?

Considerando-se que os *ransomwares* são introduzidos nos sistemas por atacantes externos e ocultos, os quais podem ser contratados na *Dark Web*, na modalidade CaaS (*Crime as a Service*), esta hipótese não pode ser descartada.

Assim, executivos mal intencionados, que desejam usar os sistemas de informação em seu trabalho para praticar atividades criminosas, podem perfeitamente contratar estes serviços com cybercriminosos externos, para simularem um ataque cibernético contra seu próprio ambiente de trabalho.

Tal classe de cybercriminosos executivos, inclusive, é denominada *insiders* pela Criminologia, que podem facilitar o acesso de sistemas corporativos a

---

[7]ATAQUE RANSOMWARE HOSPITAL. Disponível em: <https://www1.folha.uol.com.br/cotidiano/2020/07/apos-tentativa-de-ciberataque-no-sirio-libanes-setor-da-saude-teme-invasoes.shtml.> Acesso em 15.10.2020

[8]MORTE RANSOMWARE. Disponível em: https://www.cisoadvisor.com.br/ransomware-em-hospital-retardou-atendimento-paciente-morreu/>. Acesso em 15.10.2020.

estranhos. COLLIER e HUTCHINGS (2019, p.03) descrevem como agem os *insiders* corporativos

> Insiders can be committing a crime if they access data without authorisation. Insider offences include crimes committed by those who do have authorisation to the computer system, but use that access for unauthorised purposes. This can include access by employees, contractors, consultants, suppliers, and others situated within a workplace

Assim sendo, em uma primeira hipótese, quantias de origem ilícita, como produto de tráfico de drogas, poderiam estar alocadas fraudulentamente no sistema do setor financeiro da empresa, para em suposto pagamento de determinada despesa, a qual possibilite a sua oportuna movimentação, o que corresponde à etapa do *placement.*

Posteriormente, então cria-se uma situação de necessidade de pagamento de resgate em criptomoedas, para justificar o uso emergencial daquelas quantias, já alocadas no orçamento corporativo, tal qual a etapa de *layering* da lavagem de dinheiro.

Desta forma, os valores pagos, através do falso negociador, que estaria agindo a mando de dirigente da empresa, na posição de “doleiro virtual”, que irão providenciar a conversão da quantia em criptomoedas e repassa-las a cybercriminosos.

Em seguida, estes ativos seriam consequentemente circulados para *recycling*, nas *exchanges* para *wallets* (carteiras virtuais) de terceiros, os quais fariam o papel de “laranjas” dos executivos que autorizaram a liberação das quantias do resgate do ataque ransomware encomendado.

Uma segunda hipótese ainda seria a encomenda do ataque ransomware para desvio de quantias de origem lícita da empresa por executivos, em favor de terceiros, havendo a lavagem de dinheiro somente em momento posterior, com a conversão daquele valor em criptomoedas e sua consequente negociação nas *wallets* dos “laranjas”.

Vemos, então, o alto risco que a governança da empresa corre ao autorizar tais pagamentos, sem que haja políticas eficientes de gestão de risco cibernético, especialmente em caso de cyber ataques, as quais são de igual responsabilidade de seus dirigentes, sob pena de possível aplicação da teoria da cegueira deliberada àqueles que estiverem diretamente envolvidos na situação, caso seja detectada lavagem de dinheiro praticada por alguns de seus gestores.

Imagina-se, desta forma, que as autoridades do Tesouro norte-americano querem justamente coibir a prática deste ilícito financeiro, punindo os facilitadores particulares destas negociações.

Insta salientar também, a posição das empresas de seguro cibernético, nesta situação, pois este tipo de apólice usualmente cobre valores relacionados a pagamentos de resgate em ataque *ransomware*.

Com isso, também existe um risco significativo envolvido na autorização para a liberação deste valor, justamente porque tais situações podem ser simuladas, de forma semelhante a outras fraudes perpetradas para recebimento de seguros de automóveis ou de vida.

7- CONSIDERAÇÕES FINAIS

Diante de todas as considerações anteriores, conclui-se que é importante coibir a prática de pagamento de resgates em ataque cibernético *ransomware*, por conta de todas as consequências criminais envolvidas, principalmente pela possibilidade de prática dissimulada de lavagem de dinheiro, bem como evitar a intermediação de negociação destas quantias com cibercriminosos, como medida de combate ao *cybercrime.*

8- REFERÊNCIAS

DOUTRINÁRIAS

BADARÓ, Gustavo Henrique e BOTTINI, Pierpaolo Cruz. **Lavagem de Dinheiro**, São Paulo, Revista dos Tribunais, 2017, 3ª Ed

COLLIER, Ben, HUTCHINGS, Alice, **Inside out: Characterising cybercrimes committed inside and outside the workplace, Procedures** - 4th European IEEE Symposium on Security and Privacy Workshops, EUROS and PW 2019

CORDERO, Isidoro Blanco**, Negocios socialmente adecuados y delito de blanqueo de capitales, Anuario de Derecho Penal y Ciencias Penales**, vol. 50, Barcelona, 1997

ESTELLITA, Heloisa. **Criptomoedas e lavagem de dinheiro**. Resenha de: GRZYWOTZ, Johanna. Virtuelle Kryptowährungen und Geldwäsche. Berlin: Duncker & Humblot, 2019. Revista Direito GV, v. 16, n. 1, jan./abr. 2020, e1955. doi: http://dx.doi.org/ 10.1590/2317-6172201955.

KROLL, **Onde eles estão?,** Revista Digital Lec ano 8, nº 28, abril, 2020.

LLINARES, Fernando Miró, **El cibercrimen Fenomenología y criminología de la delincuencia en el ciberespacio**, Buenos Aires, Marcial Pons, 2012.

SANTOS, Humberto Mota, **O dolo de lavagem de dinheiro no Direito Penal Brasileiro em Inovações no Direito Penal Econômico – Prevenção e Repressão da Criminalidade Empresarial, Brasília**, Escola Superior do Ministério Público da União, 2018.

ELETRÔNICAS

ATAQUE RANSOMWARE HOSPITAL. Disponível em: <https://www1.folha.uol.com.br/cotidiano/2020/07/apos-tentativa-de-

ciberataque-no-sirio-libanes-setor-da-saude-teme-invasoes.shtml.> Acesso em 15.10.2020

KASPERSKY. Disponível em: <https://canaltech.com.br/seguranca/brasil-e-o-pais-mais-atingido-por-ataques-de-ransomware-na-america-latina-173018/>.Acesso em 15.10.2020.

MORTE RANSOMWARE. Disponível em: <https://www.cisoadvisor.com.br/ransomware-em-hospital-retardou-atendimento-paciente-morreu/>. Acesso em 15.10.2020

PAGAMENTO DE RESGATE EM CRIPTOMOEDAS. Disponível em: <https://www.uol.com.br/tilt/noticias/reuters/2020/10/01/tesouro-dos-eua-diz-que-empresas-podem-ser-punidas-por-pagarem-resgate-para-hackers.htm.> Acesso em 15.10.2020.

RANSOMWARE. Disponível em:<https://www.kaspersky.com.br/resource-center/definitions/what-is-ransomware>. Acesso em 15.10.2020.

SCHWARTZ, Mathew J., Ransomware: Cibercrime Public Enemy No. 1. Disponível em: <https://www.bankinfosecurity.com/blogs/ransomware-cybercrime-public-enemy-no-1-p-2952>. Acesso em 13.10.2020.

TYPOSQUATTING. Disponível em: <https://pris.com.br/blog/cybersquatting-e-typosquatting-pirataria-no-meio-digital/>. Acesso em 15.10.2020.

NORMATIVAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, NBR 27005, **Gestão de Riscos Cibernéticos**, 2011