

**JNT - FACIT BUSINESS AND TECHNOLOGY
JOURNAL ISSN: 2526-4281 - QUALIS B1**



**CRIMES CIBÉRNÉTICOS: AVANÇOS
TRAZIDOS COM A LEI CAROLINA
DIECKMAN**

**CYBER CRIMES: ADVANCES BROKEN
WITH CAROLINA DIECKMANN LAW**

**Kethelyn Bianca Pereira da Silva
FERREIRA**

**Faculdade Católica Dom Orione (FACDO)
E-mail: Kethelyn.biancaa@gmail.com**

**Daniel Cervantes Angulo VILARINHO
Faculdade Católica Dom Orione (FACDO)
E-mail:**

Danielcervantes@catolicaorione.edu.br



RESUMO

O presente artigo tem como objetivo fazer uma análise acerca dos crimes que ocorrem na Internet. Com o principal foco de analisar a referida Lei 12.737, de 30 de novembro de 2012 e quais as possíveis impunidades existentes que formam obstáculos ao combate da prática criminosa no meio digital. A pesquisa ainda investigou a diferença entre os crimes que ocorrem na rede virtual, a fim de demonstrar a problemática da ligação do criminoso foi utilizada uma metodologia qualitativa, com base em livros e artigos já publicados. Em todo o seu decorrer o artigo busca destacar a necessidade de um sistema de proteção maior de dados de usuários tanto no âmbito público quanto privado e para isso reitera que a condição de análise aqui apresentada, busca ainda analisar de que formas dispositivos de criptografia e vigilância constante podem contribuir para a fiscalização da prática de crimes em rede. Em sua parte final, o artigo busca ressaltar a importância do combate a essa prática criminosa e enfatiza os avanços que se tem tido com o combate contínuo aos crimes nas redes sociais.

Palavras-chave: Crimes Cibernéticos. Avanços. Tecnologia.

ABSTRACT

This article aims to analyze the crimes that occur on the Internet. With the main focus of analyzing the aforementioned Law 12,737, of November 30, 2012 and what possible impunity exists that form obstacles to the fight against criminal practice in the digital environment. The research also investigated the difference between crimes that occur in the virtual network, in order to demonstrate the problem of the criminal connection, a qualitative methodology was used, based on books and articles already published. Throughout its course, the article seeks to highlight the need for a greater protection system for user data both in the public and private spheres, and for that it reiterates that the condition of analysis presented here, also seeks to analyze in what ways encryption and surveillance devices can contribute to the inspection of the practice of network crimes. In its final part, the article seeks to emphasize the importance of combating this criminal practice and emphasizes the advances that have been made with the continuous fight against crimes in social networks.

Keywords: Cyber Crimes. advances. Technology.

INTRODUÇÃO

A prática de crimes na internet, especialmente em redes sociais, tem se configurado como um dos maiores problemas do mundo moderno. É recorrente encontrar em uma busca simples pela internet, uma diversidade de imagens e vídeos de conteúdo pornográfico envolvendo pessoas de todas as idades e gêneros.

Neste sentido, é importante reiterar que em um período inicial de uso da internet, sem a possibilidade de criminalização pelos atos que apresentavam teor de punibilidade para ações como as que são assistidas hoje, o que se tinha é uma total diversificação de atos que constroem suas vítimas, às vezes de forma irreparável.

O marco de mudança nesse quesito, surgiu com a promulgação da Lei 12.737, de 30 de novembro de 2012, conhecida como a Lei Carolina Dieckmann. Essa lei surgiu da necessidade de responsabilização dos envolvidos no vazamento de fotos íntimas da atriz Carolina Dieckmann, que à época do ocorrido, teve imagens íntimas vazadas em rede, e colocadas à disposição de todos na internet.

Buscando por a punição dos responsáveis por esse ato, a atriz recorreu à justiça e conseguiu com o advento dessa nova lei que promulgada em 30 de novembro de 2012, a responsabilização dos envolvidos no vazamento de suas imagens.

De modo geral, pode se dizer que a lei 12.737, dá início a uma luta constante pela regulamentação dos atos no que diz respeito ao cenário legal virtual, a criminalização de ações inapropriadas na internet, representa um avanço na segurança dos usuários que, estão à disposição de ações de cunho hediondo advindas de hackers e demais criminosos.

Com o advento dessa lei, foi aberta uma brecha para o combate a demais ações criminosas que encontravam na internet, um lugar seguro para realização de ações hediondas, e que podiam ser exercidas livremente, uma vez que a possibilidade de criminalização das mesmas era inexistente.

Dessa forma, o modelo de ação legal com foco nesse instrumento viabilizou uma série de ações que possibilitaram o enfrentamento de um problema sério e criminoso, assegurando que a internet, não seria um campo livre para ações de criminosos. Com a promulgação desse dispositivo legal, o que se conseguiu foi um alcance maior de leis que priorizavam a segurança de dados de usuários, e que criptografam dados e algoritmos, com o intuito de coibir esse modelo de ato criminoso.

A partir da determinação do termo crimes cibernéticos, o que se teve foi uma maior possibilidade de fiscalização de fontes inadequadas de imagens que expunham pessoas como se fossem mercadorias, e que, a partir do advento da lei, passaram a ser punidas e reprimidas, podendo dessa forma, proteger melhor as pessoas envolvidas nesse tipo de ação.

CONTEXTUALIZAÇÃO SOBRE A LEI CAROLINA DIECKMANN

De acordo com o entendimento de Mirabete (2017), dentro do Código Penal brasileiro, há o entendimento de que, a preservação da segurança de todos deve ser constante, para tal, utiliza-se como instrumento de combate a práticas criminosas, que ferem e prejudicam, às vezes de forma peremptória, as vítimas de tais ações.

Em Moreira (2018) se compreende que, a determinação legal sobre o combate aos crimes na internet, ganhou importantes contribuições com o advento da Lei 12,737 de 2012, conhecida como a lei Carolina Dieckmann. A partir da promulgação desse instrumento legal, a internet, outrora campo livre para a ação de criminosos, passou a ser melhor monitorada e fiscalizada, fazendo com que fosse maior a repressão a crimes como a prática de crimes.

Nos dizeres de Nucci (2019), a prática crimes virtuais se consolida como um crime hediondo tendo em vista o fato de que, a influência de suas ações alcança pontos sensíveis, ferindo no decorrer de sua formação, a autonomia sobre o seu próprio corpo, mitigando a sua dignidade sexual e também a sua dignidade como ser humano.

Nesse sentido, o que se percebe é com a promulgação da Lei 12,737 houve maior detalhamento de ações dentro do ambiente virtual e uma clara categorização do que agora se conhece como crimes cibernéticos. Observando o bojo da referida lei, se pode observar o que conta em seu texto:

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei 12.737, de 30 de novembro de 2012

Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.

Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:

“Invasão de dispositivo informático

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

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 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:

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

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal”

“Ação penal

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos”

Art. 3º Os arts. 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:

“Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública

Art. 266 [...] § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta o restabelecimento.

§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública. ” (NR)

“Falsificação de documento particular

Art. 298 [...]

Falsificação de cartão

Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito. ” (NR)

Art. 4º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.

Brasília, 30 de novembro de 2012; 191º da Independência e 124º da República (BRASIL, 2012, s/p).

Queiroz (2015) é enfático ao ressaltar que, a prática de crimes virtuais, sendo combatida investigada no ambiente virtual tem como meta a promoção de maior segurança de todos, tanto de país quanto das próprias vítimas. Desse modo, o que se consegue é obter

uma possibilidade maior de fiscalização de atos que podem reprimir a segurança de usuários de rede.

Nesse caso, é possível dizer conforme o entendimento de Reghelin (2017) que indiretamente, a lei 12.737 consegue coibir de forma indireta o aliciamento de pessoas que navegam na rede sem a presença de um adulto responsável por perto, ou que não tem uma vigilância específica.

Para Tripicchio (2017), as pratica de penalização e de combate a pornografia em rede, alcança diretamente as ações de criminosos que circulavam livremente na rede de computadores e que alcançavam pessoas que podiam ser facilmente aliciadas e envolvidas em redes de prostituição.

SEGURANÇA DE DADOS

Assim, de acordo com o Leonardi (2012), é primordial o entendimento de que as informações a respeito do usuário devem ser preservadas integralmente com o fino escopo de validar uma ação benéfica e bem ajustada de tais informações. O modo como as informações sobre os usuários são tratadas devem ser conduzidas pela ética e totalmente preservadas.

Ávila (2016) aborda que é preciso entender que a tecnologia possui sim um lado que é prejudicial ao desenvolvimento humano, para tanto, é preciso que haja uma orientação quanto à forma de utilização de recursos tecnológicos visando não somente a questão da produtividade, mas também visando o relacionamento humano que precisa estar pautado por normativas éticas e comportamentais que sustentem um convívio saudável e adequado a todos.

Neste passo, a estipulação de normas de conduta adequadas e também de cunho legal podem ser uma forma de integração amigável entre a tecnologia e as relações humanas. Posto esse fato, o autor reitera a carência legal que se tem na esfera jurídica com o intuito de nortear as relações de negócio, citando aí a relevância e acuidade da Lei Geral de Proteção de Dados Pessoais lei nº 13.709 – LGPD no que compete às formas de como a tecnologia pode ser utilizada (AVILA, 2016).

De acordo com o entendimento de Paesani (2016), a forma como as empresas lidam com os dados na atualidade, precisa ser regulamentada, tendo em vista o fato de que, com o advento tecnológico, a forma como as informações são repassadas, há que se considerar que as regulamentações no que se refere ao trato de informações de usuários, precisa

cumprir um protocolo de atuação padronizado e que seja coerente com a preservação da privacidade e da liberdade dos usuários.

Neste sentido, as regulamentações trazidas pela LGPD são notoriamente eficazes, uma vez que são minuciosas no que diz respeito à forma como as organizações devem lidar com esse tipo de informação: Ao trazer em seu artigo 4º uma clara menção quanto ao uso de informações de dados, a Lei deixa claro que:

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
I - Realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
II - Realizado para fins exclusivamente:
a). Jornalístico e artísticos; ou
b) Acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
III Realizado para fins exclusivos de:
a) Segurança pública;
b) Defesa nacional;
c) Segurança do Estado; ou
d) Atividades de investigação e repressão de infrações penais; [...]
(BRASIL, 2018, s/p).

Segundo o entendimento mostrado anteriormente, a forma como os dados são tratados, têm um escopo claro, relacionando-se ao trato negocial e econômico, não se estendendo para além disso. Ao observar a clara conotação quanto as orientações que são trazidas nessa lei, o que se constata é que a mesma, apesar de trazer a necessidade de adequação às organizações, traz fatores relevantes, no que tange à conduta no trato dos dados que estão sob o poder da organização.

Com a implantação da LGPD, as empresas certamente terão que se adequar a um novo cenário que se desenha a sua frente. Deste modo, os custos para adequação de sistema, a burocracia no que se refere à toda adaptação e ainda o envolvimento com o controle externo associado à desinformação de algumas organizações, fazem com a lei seja percebida com percepções negativas quanto à sua implantação (FRAZÃO 2018).

Dessa forma, é compreensível que o modo como as negociações acontecem no âmbito comercial comecem a passar por modificações para se adequar a sociedade que continuamente busca novas formas de viver e se relacionar. Neste passo, é prudente que se estude e compreenda estas dinamicidades sociais no viés comercial como forma de familiarizar-se com o novo cenário que se desenha a cada dia (BITTAR, 2014).

Chega-se então ao entendimento de que a tecnologia, claramente redesenhou os escopos das organizações, em praticamente todos os segmentos de atuação. Indo então ao fator mais fácil de ser exemplificado que é a divulgação de um produto, pode-se ver que,

relativo à forma de apresentação e divulgação que acontece dentro de uma ação de marketing utilizando recursos tecnológicos, é crucial que haja uma interação global entre serventia do produto e necessidade do usuário (CARNEIRO 2018).

Pode-se também dizer que o uso de tecnologia e a vasta utilização de recursos digitais enquanto fomentadores do consumo são ferramentas que carecem de certo planejamento para que tenham um efeito desejado. Não se trata simplesmente de um uso sem planejamento desta ferramenta e a obtenção automática de resultados fabulosos.

De acordo com, Souza (2013), os recursos tecnológicos que se encontram ao alcance das organizações e que são vistos como uma forma de facilitação das relações comerciais que precisam ser usados com planejamento; atendendo a objetivos gerais e específicos que condizem com a realidade da empresa e que acima de tudo, se façam úteis à população que utilizará o produto ou serviço objetivando a sua satisfação de sua necessidade.

Segundo o entendimento de Vanderlinde (2019), a compreensão do que realmente significa a satisfação do usuário abrange um leque de elementos que contemplam toda uma atuação e toda uma viabilização acerca desta. A satisfação é de modo geral, o que todo empresário, administrador ou gestor buscam, o alcance desta é dispendioso e não pode ser alcançado de uma única vez.

Portanto, a segurança de dados é uma ferramenta que contribui para a satisfação do usuário, uma vez que ela estabelece, se bem utilizada, um rápido feedback entre organização e usuário, através desse mecanismo que promove uma proximidade entre esses dois núcleos, além de proporcionar um aumento do fluxo de rotatividade e concomitantemente de negociações. No universo tecnológico/digital, é preciso validar a ideia de que a ferramenta essencial é o conhecimento, a capacidade de interação e acima de tudo, o potencial para utilizar um recurso tecnológico de forma inteligente.

Esse novo segmento profissional está relacionado ao fato das empresas estarem constantemente dispostas à adequação de metas e à reorganização de estratégias para que então se alcance os usuários. Esta definição é plausível, pois, segundo o entendimento de Vergara (2019), é preciso que, profissionais tenham como premissa profissional a certeza de que a dinamicidade é a sua principal característica e que seu usuário acima de tudo, tenha em mãos, da maneira mais ágil possível, as novas tendências e produtos lançados pelo mercado.

Para tanto, de acordo com Normandi (2019), é importante considerar que a recorrente utilização de tecnologia e ferramentas digitais dentro de organizações, apenas

reforçou a validade da opinião externa, ou seja, a tecnologia não exclui, ela integra a todos. Resumidamente, cita-se aqui os profissionais que passam informações, insights e opiniões que são, não só levadas em consideração, mas que têm de modo prático o poder de influenciar as decisões e afetar – positiva ou negativamente – o poder de compra de uma usuáriuola. Indispensável dizer que estes profissionais têm tido uma grande importância nas relações de comércio na atualidade.

Ao voltar a percepção para a implantação da LGPD, é necessário, de acordo com o pensamento de França, Faria, Rangel e Oliveira (2018), que se observe que mesmo apresentando algumas desvantagens no seu âmbito inicial, especialmente no que se refere à todo o processo de adaptação, são notórias as suas vantagens.

Doneda (2018), cita que dentre os fatores vantajosos, encontra-se a segurança no tratamento de dados, deste modo, o autor evidencia o fato de que, as ações criminosas no espaço virtual estão cada vez mais frequentes. Entre os itens que podem ser roubados neste ambiente, as informações pessoais de pessoas comuns são recursos valiosos que podem gerar inúmeros rendimentos, quando utilizados de forma inadequada. Com isso, a segurança promovida pela nova LGPD, pode trazer à empresas, a oportunidade de se resguardar, de atualizar suas políticas de privacidade e preservar informações relevantes de seus usuários.

Conforme se vê em Freitas e Pamplona (2018), o enquadramento organizacional das cooperativas de saúde com a implantação do sistema ERP e de acordo com os ditames da LGPD, trazem à empresa maior confiabilidade do usuário em relação às suas ações, trata-se de uma oportunidade de fazer com que o usuário compreenda que suas informações estão sendo cuidadas de modo criterioso e em acordo com os fundamentos legais.

Importante dizer ainda, segundo Cavalcanti e Santos (2018), com o advento dessa nova lei, o que se descortina diante do corpo empresarial, é uma realidade que não pode ser mais mudada, tendo em vista os constantes avanços e as recorrentes adequações tecnológicas, por quais todos passam, é saudável o surgimento de uma nova lei que proteja de modo direto as informações de usuários.

Em linhas gerais, pode-se dizer que sim, a lei é vantajosa e dá ao usuário a vantagem de repasse de dados com a garantia de que suas informações serão repassadas de modo ordenado e terão uma utilização específica. Quanto à organização, fica a clara possibilidade de enquadramento no novo cenário que se desenha.

De acordo com o entendimento de Ebberts e Van Dijk (2017), é imprescindível que se tenha em todo ordenamento jurídico do globo, um instrumento de regulamentação quanto ao uso de informações de usuários. Ao se trazer a questão especificamente para o caso das instituições, há que se levar em conta o fato de que, sem a devida proteção de dados cadastrais de usuários, é possível e passível o repasse de informações sem a menor dificuldade por parte da operadora, prejudicando assim o usuário de uma forma violenta.

Horrigan (2019), em sua abordagem, reflete o fato de que, a troca de dados entre usuários e empresas nos dias atuais, não pode mais ser conduzida somente pela boa-fé entre as partes, é vital que haja um processo de orientação e de normatização quanto ao uso de informações pessoais, sob de se tornar o sequestro de dados, o uso inapropriado de informações e o mal-uso destas, uma constante na vida de todos.

Junior (2019) ao falar sobre tal situação, acresce ainda que, os fatores de prevenção, responsabilização e prestação de contas, segurança e qualidade dos dados, mostram resumidamente, o quão delicado é o trato com dados de terceiros. O autor explica ainda que, sem uma normativa que de fato oriente a conduta de empresas em relação ao modo como lida com informações repassadas por usuários, o que se teria, seria uma verdadeira anarquia quanto à utilização desregrada e infundada de dados pessoais.

Ao se seguir na análise do que é disposto na lei que é objeto de estudo deste artigo, encontra-se em seu artigo 7º o seguinte exposto:

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - Mediante o fornecimento de consentimento pelo titular;

II - Para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; [...] (BRASIL, 2018, s/p).

O artigo 7º exposto acima, explana as ocasiões em que os dados fornecidos por usuários podem ser compartilhados, ao numerar essas possibilidades, o que se tem é um claro fator normatizador nestas relações. Ainda no tocante à demais especificações trazidas por essa lei, pode-se ver em seu artigo 9º o seguinte exposto:

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - Finalidade específica do tratamento;

II Forma e duração do tratamento, observados os segredos comercial e industrial;

III Identificação do controlador;

IV Informações de contato do controlador; (BRASIL, 2018, s/p).

Deste modo, há que se considerar que o essencial neste caso, é que as instituições, estruturarem e organizem treinamentos e formas de orientação, com o objetivo de se adequar a tal orientação legal, fazendo desta forma, que sejam cumpridos todos os ditames promulgados em lei, evitando assim descumprir o que já é promulgado como fator complementar do direito de privacidade do usuário.

Em Vanderline (2019), se encontra a definição de que, no que se refere ao trato de informações de usuários por empresas, especificamente as instituições, é preciso levar em conta que, as instituições, já seguem uma normativa própria referente à ética, que resguarda informações quanto ao histórico médico, zelando pela integridade de cada um.

Assim, Vanderline (2019) segue dizendo que a LGPD tende a trazer sim mudanças no que se refere ao trato geral de informações de usuários das instituições, no entanto, de acordo com o próprio autor, trata-se de uma ação que visa somente o melhoramento do cuidado das instituições em relação à estes dados.

Assim, em seu artigo 1º e 2º pode-se ler que:

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. (Incluído pela Lei nº 13.853, de 2019). Vigência

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: (BRASIL, 2018, s/p).

Conforme se tem esboçado no artigo 1º da Lei nº 13.709, de 14 de agosto de 2018, o ideal de sua promulgação consiste em proteger os direitos fundamentais de liberdade e privacidade, bem como do livre desempenho de uma personalidade. No caso de uma instituição qualquer, é preciso considerar que, ao repassar as informações pessoais, um usuário tem como objetivo apenas o preenchimento cadastral, não se trata da criação de um

vínculo no qual a cooperativa tem o pleno direito de usar as informações que lhe são repassadas de forma plena.

Ao analisar de modo cuidadoso o bojo da lei nº 13.709, de 14 de agosto de 2018. Chega-se ao entendimento que seu escopo central se refere à segurança dos dados que são repassados pelo usuário. Trata-se na verdade de um sistema que ambiciona a proteção de informações que, se utilizadas de forma equivocada, podem provocar efeitos negativos de todos os usuários, nesta senda, há que se levar em conta o fato de que essa normativa, se refere à um campo geral, e não especificamente direcionado às instituições de modo geral.

As especificidades que a lei traz se referem ao fato de que a necessidade de adequação é clara e a mesma carece de articulação e organização por parte da equipe de gestão da instituição. Essa necessidade se refere ao fato de que, por ser a lei um instrumento regulador de ações, é viável que a empresa, a fim de cumprir com todos os posicionamentos que são expostos no instrumento legal, possa recrutar seus colaboradores no intuito de tornar familiar à estes, todas as formas de lidar com esse novo tipo de orientação.

Os fatores como a liberdade e a privacidade, precisam continuar a ser itens de valor máximo para uma pessoa. Deste modo, mesmo em uma operação onde seus dados sejam acessados com frequência e com facilidade, pelas empresas que com ele negociam, é vital que a sua privacidade seja preservada e que os fatores relativos à transação realizada, permaneçam sob os interesses de usuário e organização.

Deste modo, a necessidade de adequação das instituições às atualizações trazidas com a implantação da LGPD de fato requer da organização um bom enquadramento quanto à capacidade da organização em lidar com as novas regulamentações, além disso, todo o processo de adaptação irá exigir tanto empenho físico, quanto de ordem financeira, investidos em adaptação e aprendizagem com o fim de fazer com que tudo de organize de forma clara.

De acordo com a percepção de Dunaigre (2019), é necessário que se compreenda que a efetividade das ações de combate à crimes virtuais, decorrentes de ações policiais que investigam e punem criminosos que até pouco tempo agiam de forma livre na internet, tem feito com que resultados satisfatórios sejam alcançados no combate a essa prática criminosa.

Zaniolo (2017) em sua consideração sobre crimes modernos praticados em decorrência do efeito da tecnologia, expõe que a prática de crimes virtuais ganhou contornos bizarros com o advento da internet. O autor explica que, o antes já era assustador

passou a ser praticado em rede de forma quase aberta ainda nos primórdios da internet. Ações que tinham como escopo a penalização dessas ações esbarravam na ausência de dispositivos que enquadravam corretamente tais ações.

CONSIDERAÇÕES FINAIS

Ao se alcançar a finalização desse trabalho, alcança-se pontos relevantes de compreensão que expõem a indispensabilidade de dispositivos legais que coíbem e combatem a prática criminosa nas redes sociais. Considerando a motivação de disposição desse dispositivo legal, se compreende que inicialmente, a sua promulgação nasceu para a proibição ou coibição da disponibilidade de imagens íntimas em redes sociais.

Mesmo assim, se alcançou com a disponibilidade desse instrumento legal, a oportunidade de combater ações tão prejudiciais e maledicentes que comprometiam a imagem de muitas pessoas que eram expostas de forma criminosa e tratadas como mercadorias nas redes sociais. Objetos de desejo de pessoas adultas que buscavam saciar vontades insanas com pessoas indefesas.

O combate aos crimes virtuais representou com a promulgação de leis que reprimem ações dessa natureza e que ajuda na proteção de dados do usuário, um avanço na legalização sobre o que ocorre no ambiente virtual, já considerado como um campo livre para ações que no plano real, são combatidas vorazmente por autoridades.

Nesse sentido, pode se dizer que com o avanço legal que criminaliza ações dentro do ambiente virtual, o que se consegue é uma normatização capaz de fazer com que a comunidade que faz uso constante de redes sociais tenha maior segurança e melhor fluidez em suas ações, uma vez que pode compreender que a sua segurança está respaldada por um dispositivo legal de fato eficiente e alinhado com os escopos apresentados no Código Penal.

Ferreira (2019) explica que, com o avanço de leis de criminalização como a Lei Carolina Dieckmann e com a possibilidade de maior proteção de dados com a promulgação da LGPD, o que se teve foi uma maior segurança no uso de internet, uma vez que a possibilidade de criptografia de dados e maior responsabilização no uso destes, deixou em aberto a possibilidade de engajamento de combate a crimes em redes, uma vez que obriga a organizações um maior cuidado com os dados de seus usuários e pune ações de vazamento indevido.

Serafim (2019) reitera ainda que, a prática de crimes virtuais se consolida um problema vergonhoso em uma sociedade que se diz evoluída, mas que ainda precisa lidar

com o recorrente fluxo e notificações de pessoas abusadas, violentadas e expostas de forma indevida em redes sociais.

Importante ainda dizer que de acordo com o entendimento de Hare (2016), sem a promulgação de leis e demais dispositivos de proteção, o ambiente virtual que atualmente se conhece, seria na verdade um modelo de lugar hostil onde criminosos podiam atuar livremente e com a certeza de que não haveria punição para seus crimes. Nesse caso, se observa que com o advento da Lei 12.737, foi aberto um importante caminho para a promulgação de demais dispositivos que tem como escopo a proteção de dados de usuários e que podem de modo direto, contribuir na devida penalização de criminosos que viam na internet um ambiente livre para ação de suas práticas violentas contra usuários.

REFERÊNCIAS

ÁVILA, Humberto. **Teoria dos princípios: da definição à aplicação dos princípios jurídicos**. 6. ed. São Paulo: Malheiros, 2016.

AVOLIO, Luiz Francisco Torquato. **Provas Ilícitas**. São Paulo: Revista dos Tribunais, 1995.

BECKER, Howard. **Outsiders: Estudos de Sociologia do Desvio**. São Paulo, Zahar, 2018.

BITTAR, Carlos Alberto. **Os direitos da personalidade**. 7. ed. Rio de Janeiro: Forense Universitária, 2014.

BRAGA, Sidney da Silva. **Iniciativa probatória do juiz no processo civil**. São Paulo: Saraiva, 2004.

BRASIL: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm acesso em 19 de maio de 2022.

BRASIL: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm acesso em 18 de maio de 2022.

BREIER, Ricardo.; TRINDADE, Jorge. **Aspectos psicológicos e penais**. Porto Alegre, Livraria do Advogado, 2018

CANOTILHO, César Dario Mariano da. **Provas Ilícitas**. 3ª ed. Rio de Janeiro: Forense, 2010.

CARNEIRO, José Luís. Breve história do computador. 2018. Disponível em: www.scielo.com.br acesso em 19 de maio de 2022.

CAVALCANTI, Natália Peppi; SANTOS, Luiza Mendonça da Silva Belo. **A Lei Geral de Proteção de Dados do Brasil na era do Big Data**. In Tecnologia Jurídica & Direito

Digital - II Congresso Internacional de Direito, Governo e Tecnologia. 2018. Acesso em 05 de março de 2021

COMPARATO, José. **Fundamentos Principiológicos do Processo Civil**. Rio de Janeiro: Forense, 2013.

DONEDA, Danilo. **Proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. Brasília: SDE/DPDC. 2018.

DUNAIGRE, Patrice. **O ato criminoso na história da sexualidade humana**. In: INOCÊNCIA em perigo/abuso sexual, pornografia na Internet. Rio de Janeiro: UNESCO/Abranet/Garamond, 2019

EBBERS. W.E. VAN DIJK. J.A.G.M. **Resistance and support to electronic government, building a model of innovation**. Government Information Quarterly 24 (2017) 554–575

ESCUADERO ALDAY, Humberto. **Curso de Direito Processual Civil**. Volume I, 42ª ed. Rio de Janeiro: Forense, 2012.

FERREIRA, Aurélio Buarque de Hollanda. **Dicionário Aurélio eletrônico: século XXI. Versão 3.0**. Rio de Janeiro: Nova Fronteira. Desenvolvido por MGB Informática, 2019.

FINKELHOR, David. **Explanations of Pedophilia: a four factor model**. [S.l.], 2016. Disponível em: http://www.jstor.org/stable/3812437?seq=1#page_scan_tab_contents acesso em 19 de maio de 2022.

FRANÇA, T. C.; FARIA, F. F.; RANGEL, F. M.; FARIAS, C. M.; OLIVEIRA, J. Big Social Data: Princípios sobre coleta, tratamento e análise de dados sociais. Artigo publicado nos anais do XXIX Simpósio Brasileiro de Banco de Dados (SBBBD) 2018. **Curi-Revista Jurídica da Escola Superior de Advocacia da OAB-PR** Ano 4 - Número 1 - Maio de 2019. p. 8. Disponível em: <http://www.inf.ufpr.br/sbbdsbsc2014/sbbd/proceedings/artigos/pdfs/127.pdf>. Acesso em 05 de maio de 2021

FRAZÃO, Ana. **Nova LGPD: principais repercussões para a atividade empresarial** 2018. Disponível em www.jusbrasil.com.br acesso em 05 de maio de 2021

FREITAS, Cinthia Obladen de Almendra; PAMPLONA, Danielle Anne. **A complexa relação entre negócios e direitos humanos: as violações dos direitos de personalidade por meio de Tracking e Profiling em serviços online**. 2018 Disponível em www.jusbrasil.com.br acesso em 19 de maio de 2022.

GRECO FILHO, Vicente. **Direito Processual Civil Brasileiro**. Volume 2, 14ª ed. rev. atual. São Paulo: Saraiva, 2000.

GRUBER, Theotonio. **Código de Processo Civil e Legislação Processual em Vigor**. 35ª ed., atual. São Paulo: Saraiva, 2013.

HÄBERLE, De Plácido e. **Vocabulário Jurídico**. 18ª ed. Rio de Janeiro: Forense, 2001.

Kethelyn Bianca Pereira da Silva FERREIRA; Daniel Cervantes Angulo VILARINHO. CRIMES CIBÉRNÉTICOS: AVANÇOS TRAZIDOS COM A LEI CAROLINA DIECKMAN. JNT- Facit Business and Technology Journal. QUALIS B1. AGOSTO-OUTUBRO/2022. Ed. 39 Vol.3. Págs. 279-294. ISSN: 2526-4281 <http://revistas.faculdefacit.edu.br>. E-mail: jnt@faculdefacit.edu.br.

HARE, R. D. **Psychopathy: a clinical and forensic overview**. Psychiatr Clin North Am., Philadelphia, v. 29, n. 3, p. 709-24, 2016.

HENRIQUES, Ana; PEREIRA, Ana Cristina. **Pais não terão acesso livre a registro de agressores sexuais de menores**. Público, [Lisboa], 13 de mar. 2015. Disponível em: <http://www.publico.pt/sociedade/noticia/governo-aprova-registo-de-agressores-sexuais-1688931> acesso em 19 de maio de 2022.

HERTEL, Gilmar Ferreira et al, **Curso de Direito Constitucional**, São Paulo: Saraiva: 2006

HORRIGAN. John B. **Americans Fall Along a Spectrum of Preparedness When it Comes to Using Tech Tools to Pursue Learning Oline, And Manys Are Not Eager Or Ready To Take The Plunge**. Pew Research Center – Numbers, Facts and Trends Shaping the World. 2019

JUNIOR: Wagner Coppede. **Transformação Digital na Política Pública**. Fundação Getúlio Vargas - Escola De Administração De Empresas De São Paulo. S.P. 2019

LEONARDI, Marcel. **Tutela e privacidade na internet**. 1ª ed. São Paulo: Saraiva, 2012.
MACHADO, Antônio Cláudio da Costa. **Código de Processo Civil Interpretado**. 4ª ed. rev., atual. São Paulo: Manole, 2004.

MIRABETE, Julio Fabbrini. **Código Penal Interpretado**. São Paulo. Atlas S/A. 2017.
MONNERAT, Carlos Fonseca. **A inversão do ônus da prova no processo penal**. Santos, São Paulo: Comunnicar, 2006.

MOREIRA, Ana Selma. **Aspectos jurídicos e sociais**. Cronus, 2018.

MORESCO, José Carlos Barbosa. **O novo processo civil brasileiro**. 25ª ed., rev., atual. Rio de Janeiro: Forense, 2015.

NORMANDI, Carolina. **Direito à intimidade do empregado X direito de propriedade e poder diretivo do empregador**. Síntese Jornal, Porto Alegre, v. 5, n. 56, out. 2019, p. 9-15.

NOVELINO, Antônio Cláudio da Costa. **Código de Processo Civil Interpretado**. 4ª ed. rev., atual. São Paulo: Manole, 2008.

NUCCI, Guilherme Silva. **Crimes contra a dignidade sexual**. São Paulo, Revista dos Tribunais, 2019.

PAESANI, Liliana Minardi. **Direito e internet**. 5ª ed. São Paulo: Editora Atlas S.A., 2016.

QUEIROZ, Paulo de Souza. **Penas e medidas de segurança se distinguem realmente?** Boletim IBCCRIM. São Paulo, n.147, 2015.

REALE: Miguel. **Democracia, liberdade, igualdade: os três caminhos**. 2ª ed. São Paulo: Saraiva, 2010.

Kethelyn Bianca Pereira da Silva FERREIRA; Daniel Cervantes Angulo VILARINHO. CRIMES CIBÉRNÉTICOS: AVANÇOS TRAZIDOS COM A LEI CAROLINA DIECKMAN. JNT- Facit Business and Technology Journal. QUALIS B1. AGOSTO-OUTUBRO/2022. Ed. 39 Vol.3. Págs. 279-294. ISSN: 2526-4281 <http://revistas.faculdefacit.edu.br>. E-mail: jnt@faculdefacit.edu.br.

REGHELIN, Elisangela Melo. **Crimes Sexuais Violentos: tendências punitivas**. Porto Alegre, Livraria do Advogado, 2017.

SARLET, José Frederico. **Manual de Direito Processual Civil**. Volume 1, 5ª ed.. São Paulo: Saraiva, 2013.

SERAFIM, Antonio de Pádua et al. **Perfil psicológico e comportamental de agressores sexuais**. São Paulo: Faculdade de Medicina da Universidade de São Paulo (FMUSP), ano. Disponível em: <http://urutu.hcnet.usp.br/ipq/revista/vol36/n3/pdfs/105.pdf> acesso em 19 de maio de 2022.

SOUZA, Marco Antônio Scheuer de. **O dano moral nas relações entre empregados e empregadores**. Erechim: Edelbra, 2013.

TEIXEIRA, Rogério Lauria. **Princípios e regras orientadoras do novo processo penal brasileiro**. Rio de Janeiro: Forense, 2011.

TRIPICCHIO, Adalberto. Sexologia Forense. Psicologia – RedePsi, [S.l.], 13 jun. 2017.

VANDERLINDE, Marcelo Ivo Melo. **Da Tecnologia**: Disponível em: <<http://www.clubjus.com.br/?artigos&ver=2.25667&hl=no>>.2019

VERGARA, Andrew J. **Fundamentos do Comportamento Organizacional**. Editora Cengage, Ano 2019.

ZANIOLO, Pedro Augusto. **Crimes modernos: o impacto da tecnologia no direito**. Curitiba: Juruá, 2017.