VII ENCONTRO VIRTUAL DO CONPEDI

DIREITOS E GARANTIAS FUNDAMENTAIS II

THAIS JANAINA WENCZENOVICZ

DIOGO DE ALMEIDA VIANA DOS SANTOS

D597

Direitos e garantias fundamentais II [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Diogo De Almeida Viana Dos Santos; Thais Janaina Wenczenovicz – Florianópolis: CONPEDI, 2024.

Inclui bibliografia
ISBN: 978-85-5505-896-7
Modo de acesso: www.conpedi.org.br em publicações
Tema: A pesquisa jurídica na perspectiva da transdisciplinaridade

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direitos. 3. Garantias fundamentais. VII Encontro Virtual do CONPEDI (1: 2024 : Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

VII ENCONTRO VIRTUAL DO CONPEDI

DIREITOS E GARANTIAS FUNDAMENTAIS II

Apresentação

DIREITOS E GARANTIAS FUNDAMENTAIS II

Com muita satisfação, apresentamos à comunidade acadêmica os resultados de estudos e discussões aprovados para o VII ENCONTRO VIRTUAL DO CONPEDI, realizado entre os dias 24 e 28 de junho de 2024. Esta obra científica é destinada à difusão de temas contemporâneos, sob a linha estruturante "Constitucionalismo, Desenvolvimento, Sustentabilidade e Smart Cities".

Os frutíferos debates do Grupo de Trabalho "Direitos e Garantias Fundamentais II" se deram em subgrupos temáticos, com interações voltadas à disseminação e aperfeiçoamento do conhecimento produzido por pesquisadores das mais diversas regiões do Brasil, no âmbito de Programas de Mestrado e Doutorado em Direito e áreas afins utilizando-se do ambiente de teletransmissão em videoconferência, com o fim de propiciar a democratizaçnao do acesso às frutíferas e proveitosas discussões, deste que já se tornou o maior fórum de debates científicos na área do Direito no Brasil e na América Latina.

Os trabalhos apresentados, que ora compõem este registro, testemunham a utilidade do compartilhamento e disseminação do conhecimento e ideias inovadoras que contribuem para o desenvolvimento da ciência jurídica e afirmação da justiça no Brasil, Américas e Mundo.

Congratulamos a grande comunidade que compõe o Conselho Nacional de Pesquisa e Pós-Graduação em Direito por seu contínuo esforço de prover um ambiente e oportunidades de aprimoramento da academia jurídica nacional.

Thais Janaina Wenczenovicz

UNIVERSIDADE ESTADUAL DO RIO GRANDE DO SUL/UNIVERSIDADE DO OESTE DE SANTA CATARINA

Diogo de Almeida Viana dos Santos

Universidade Estadual do Maranhão - UEMA, e Universidade UNICEUMA

- Grupo temático 1

A PROTEÇÃO DOS DIREITOS FUNDAMENTAIS DIANTE DA OBSERVÂNCIA DO PRINCÍPIO DA PROPORCIONALIDADE - Tassiane Ferreira Cardoso , Karen Beltrame Becker Fritz;

BASE AXIOLÓGICA DOS DIREITOS FUNDAMENTAIS DO PASSADO AO FUTURO: DA DIMENSÃO PSICOFÍSICA A VIRTUAL - Mariely Viviani Cacerez;

EFICÁCIA DOS DIREITOS FUNDAMENTAIS E CONSTITUCIONALIZAÇÃO DO DIREITO PRIVADO - Patrícia Maria Barreto Bellot de Souza;

VULNERABILIDADES E PROTEÇÃO SOCIAL: POLÍTICAS DE ASSITÊNCIA NA PROMOÇÃO DOS DIREITOS HUMANOS - Anna Paula Bagetti Zeifert , Vitória Agnoletto;

A FORÇA DO PRINCÍPIO DA DIGNIDADE DA PESSOA HUMANA NAS NOVAS RELAÇÕES DE TRABALHO E NA CRISE SINDICAL NO BRASIL - Marcel Carlos Lopes Félix , Joao Antonio de Oliveira Pereira , Bruna Silveira Roncato Aguiar.

Grupo temático 2

TRABALHO PARA PESSOAS COM DEFICIÊNCIA E AGENDA 2030: ANÁLISE DO PROJETO DE LEI DO SENADO N° 3461, DE 2023 - Luciana Cristina de Souza , Beatriz Moreira Federici;

A TUTELA JURISDICIONAL PARA GARANTIA DAS COTAS E AÇÕES AFIRMATIVAS RACIAIS - Jônatas Luiz Moreira de Paula , Reginaldo Bonifacio Marques;

ESCRAVIDÃO MODERNA: SOB A ÓTICA DA HERANÇA DA COLONIZAÇÃO - Rafiza Soares Teixeira Nunes;

IGUALDADE SALARIAL ENTRE HOMENS E MULHERES E O SUPERENDIVIDAMENTO DA CONSUMIDORA - Ana Cláudia Rodrigues De Faria , Samantha Ribeiro Meyer-pflug;

APONTAMENTOS PARA UMA POLÍTICA PÚBLICA ANTIDISCRIMINATÓRIA MENOS TÍMIDA: DIRIGISMO MORAL E PERSISTÊNCIA AUTORITÁRIA NA ADPF 291 - Mario Cesar da Silva Andrade.

Grupo temático 3

CONSTITUCIONALISMO E CIDADANIA: CONSIDERAÇÕES AO RECONHECIMENTO DE DIREITO DAS PESSOAS SURDAS À EDUCAÇÃO BILINGUE NA ERA DIGITAL EM MANAUS - Déborah Costa de Souza , Roger Luiz Paz de Almeida;

PROMOVENDO A EDUCAÇÃO INCLUSIVA: O PAPEL DO MINISTÉRIO PÚBLICO NA EFETIVAÇÃO DA EDUCAÇÃO BÁSICA PARA TODOS - Renata Nazareno Monteiro Pereira da Silva;

DADOS SENSÍVEIS E REGISTRO DE IMÓVEIS: A ADEQUAÇÃO DAS SERVENTIAS EXTRAJUDICIAIS À LEI GERAL DE PROTEÇÃO DE DADOS - Viviane Freitas Perdigao Lima , Ana Josina Silva Cardoso de Oliveira;

OS EFEITOS DO RE Nº 865.401/MG NA REQUISIÇÃO DE INFORMAÇÕES PÚBLICAS PELOS DEPUTADOS ESTADUAIS DO MARANHÃO: ANÁLISE COMPARATIVA ENTRE OS ANOS DE 2015 E 2023 - Marco Aurélio Rodrigues da Cunha e Cruz , Alex Bruno Canela Vilela;

LEI GERAL DE PROTEÇÃO DE DADOS NAS SERVENTIAS EXTRAJUDICIAIS: PUBLICIDADE REGISTRAL X PRIVACIDADE - Aryala Stefani Wommer Ghirotto , Renata Capriolli Zocatelli Queiroz , Luis Frederico De Medeiros Portolan Galvao Minnicelli;

VAZAMENTO DE DADOS PARA DEEP WEB E O DIREITO À PRIVACIDADE SOBRE A ÓTICA DA LGPD - Soraia Giovana Ladeia Forcelini , Jéssica Amanda Fachin.

Grupo temático 4

DIREITOS HUMANOS E DIREITOS FUNDAMENTAIS: DEFINIÇÕES E LIMITES JURÍDICOS APLICADOS NO CONTEXTO DA PANDEMIA DE COVID-19 - Wellington Aparecido Prado Carvalho , Jaime Domingues Brito , Tiago Domingues Brito;

INTERDEPENDÊNCIA ENTRE OS OBJETIVOS DE DESENVOLVIMENTO SUSTENTÁVEL: O PAPEL DO ACESSO À ÁGUA POTÁVEL NOS ESFORÇOS GLOBAIS DE SUSTENTABILIDADE - Raquel Magali Pretto dos Santos;

O ACORDO DE NÃO PERSECUÇÃO PENAL COMO GARANTIDOR DE DIREITOS FUNDAMENTAIS DO ACUSADO E O REFLEXO NO ORÇAMENTO PÚBLICO - Raphael Penha Hermano , Marcio Pereira Dias;

O ESTADO DE COISAS INCONSTITUCIONAL DECORRENTE DA SUPERLOTAÇÃO PRISIONAL BRASILEIRA – ANÁLISE SOBRE A ADPF 347 - Carlos Antônio Sari Júnior , Franciele Lippel Laubenstein , Raphael Quagliato Bellinati;

PRESUNÇÃO DE INOCÊNCIA: FORMA DE MUTAÇÃO DE PRECEDENTES E A PRISÃO AUTOMÁTICA NO JÚRI - Rafael Corrêa Dias Pinto Carlos , Krishina Day Carrilho Bentes Lobato Ribeiro.

VAZAMENTO DE DADOS PARA DEEP WEB E O DIREITO À PRIVACIDADE SOBRE A ÓTICA DA LGPD

DATA LEAKAGE TO THE DEEP WEB AND THE RIGHT TO PRIVACY FROM THE PERSPECTIVE OF LGPD

Soraia Giovana Ladeia Forcelini
Jéssica Amanda Fachin

Resumo

O vazamento digital é uma preocupação frequente nos dias de hoje, principalmente em relação às empresas que detém grande volume de informações sobre seus clientes. Cabe destacar o papel importante da lei geral de proteção de dados a trazer maior segurança para os usuários, tendo como principal foco de atuação os dados sensíveis que, as pessoas possuem relacionados à vida particular e que podem invariavelmente ser atacados, posto que, o bem mais precioso, não está petróleo, ouro, pedras preciosas, ou qualquer outro meio valioso que se utilizavam antigamente, mas sim, os dados pessoais. A metodologia utilizada na presente pesquisa e a dedutiva, por meio de seleção de dados, pode significar diversas mudanças no país, como exemplo de algumas empresas que influenciaram na tomada de decisões, que tornaram-se evidentes no Reino Unido optando desvincular da União Europeia, conhecido como Brexit e também a eleição para a presidência dos Estados Unidos onde Donald Trump se elegeu, onde ambos contaram com a empresa Cambridge Analytica. Logo, a problema dos vazamentos de dados sendo eles disfarçados de cooperação, pesquisa de opinião, ou outro artifício que possa ser utilizado para coletar informações de pessoas, ou aquelas que já se encontram em um determinado servidor, oferecidos gratuitamente, são um objeto de estudo para ser analisado, uma vez que essas informações podem significar a mudança do rumo de uma história. Assim, o presente trazer como resultado principal, evitar o mau uso das informações, evitando assim a violação da integridade do cidadão.

Palavras-chave: Deep web, Vazamento, Lgpd, Dados, Privacidade

Abstract/Resumen/Résumé

Digital leakage is a frequent concern nowadays, especially concerning companies holding large volumes of customer information. It's worth highlighting the significant role of the general data protection law in providing greater security for users, focusing primarily on sensitive data individuals possess regarding their private lives, which can invariably be targeted. This is because the most precious asset today is not oil, gold, or gems, as in ancient times, but personal data. The methodology employed in this research is deductive, through data selection, potentially signifying various changes in the country. For instance, certain companies influenced decision-making, evident in the UK's decision to exit the European Union, known as Brexit, and in the US presidential election where Donald Trump won, both

involving Cambridge Analytica. Consequently, the issue of data leaks, whether disguised ascooperation, opinion polls, or other means to collect personal information, including those already stored on servers and offered for free, warrants thorough examination. Such information can alter the course of history. Therefore, the main outcome sought is to prevent the misuse of data, thereby safeguarding citizens' integrity.

Keywords/Palabras-claves/Mots-clés: Deep web,, Leak,, Lgpd, Data, Privacy

INTRODUÇÃO

O presente estudo adota uma abordagem metodológica que combina análise quantitativa e qualitativa para investigar os vazamentos de dados na Deep Web. Seu principal objetivo é abordar a preocupante questão do uso indevido das informações pessoais dos cidadãos, visando expor resultados relevantes que possam informar a formulação de novas medidas jurídicas capazes de prevenir efetivamente a violação dos direitos humanos por meio desses meios eletrônicos.

Com o advento da internet, testemunhamos uma notável ascensão na aceitação e integração dos computadores nos ambientes profissionais. Inicialmente encantadas pela ideia de possuir um dispositivo capaz de aprimorar suas atividades diárias, as pessoas gradualmente aumentaram sua dependência desses dispositivos tanto em casa quanto no trabalho, à medida que a internet se expandia. O avanço tecnológico não apenas conferiu funcionalidade aos computadores no ambiente de trabalho, mas também os inseriu mais profundamente em nossas vidas pessoais. A conexão à internet tornou-se uma necessidade essencial, impulsionando a demanda por dispositivos pessoais para acessar recursos online. Esse processo não apenas aumentou a familiaridade das pessoas com os computadores, mas também sua dependência para facilitar diversas tarefas e comunicações.

Essa evolução não ficou restrita ao âmbito profissional, estendendo-se ao contexto doméstico, onde os computadores se tornaram praticamente indispensáveis para uma variedade de atividades cotidianas, desde comunicação até entretenimento e educação. Tal transição reflete não apenas avanços tecnológicos, mas também mudanças nas necessidades e expectativas das pessoas em relação à conectividade e ao acesso instantâneo à informação.

Assim como os televisores, que gradualmente se estabeleceram nos lares, os computadores seguiram uma trajetória similar, ampliando consideravelmente sua presença nos espaços domésticos. Paralelamente, a popularidade dos dispositivos móveis cresceu exponencialmente, especialmente no contexto brasileiro, tornando-se quase um fenômeno cultural e contribuindo para a universalização do acesso à internet.

Essa disseminação massiva da tecnologia não apenas ampliou o acesso, mas também estabeleceu um novo padrão de interconexão digital, onde os computadores são vistos como ferramentas essenciais para atividades cotidianas. Com a expansão dos dispositivos móveis, a presença e a utilidade dos computadores não foram substituídas, mas sim complementadas, resultando em uma integração mais ampla e dinâmica entre diferentes plataformas tecnológicas.A transformação dos computadores em um elemento indispensável na vida

cotidiana também é reflexo da evolução tecnológica e das demandas crescentes por conectividade e acesso à informação. Esta interligação entre os dispositivos, ao invés de eliminar o espaço dos computadores, apenas consolidou sua importância, tornando-os peças-chave na experiência digital contemporânea, oferecendo recursos e possibilidades que se complementam com os dispositivos móveis.

Com a expansão da internet, a integração desta com os dispositivos móveis, como os celulares, tornou-se indispensável para seu pleno funcionamento. Desde o momento inicial de ligar o aparelho, os usuários são confrontados com a exigência de fornecer seus dados pessoais, essenciais para iniciar e personalizar o uso do dispositivo. Esse procedimento é comum para garantir funcionalidades completas e acesso a serviços diversos, refletindo a importância dos dados na atualidade para personalização e acesso a recursos exclusivos.

Ao iniciar o uso das redes sociais, é comum criar contas e fornecer dados sensíveis, como nome, e-mail e data de nascimento, para acessar as vantagens da plataforma. Esse processo envolve compartilhar informações pessoais, associadas à possibilidade de desfrutar de recursos exclusivos e interações personalizadas.

Entretanto, muitos usuários, movidos pelo entusiasmo, aceitam os termos propostos pelas plataformas sem ler todo o contrato, resultando na concessão involuntária de seus direitos privados. Essa prática destaca a urgência de conscientização sobre a importância da leitura atenta desses contratos e da transparência das plataformas digitais na apresentação desses termos. Com o advento da Lei Geral de Proteção de Dados, os sítios eletrônicos trazem questões sobre o uso de cookies para dar acesso aos usuários. Problemas como a falta de compreensão dos cookies e a recusa de empresas em fornecer informações protegidas pela legislação destacam a complexidade da proteção de dados na era digital.

Em resumo, a crescente integração dos computadores, especialmente dispositivos móveis, no ambiente profissional e pessoal é impulsionada pelo progresso tecnológico e pela necessidade de conectividade. A questão da privacidade dos dados pessoais na era digital é crucial, ressaltando a importância da conscientização dos usuários e de regulamentações claras para proteger a privacidade individual.

Quando tais conteúdos são liberados, a plataforma pode atribuir valor a eles para sua própria utilização, sem enfrentar sanções adequadas, o que, por sua vez, pode resultar em diversos problemas relacionados ao uso indiscriminado de dados sensíveis. Essas questões ressaltam a complexidade das leis de proteção de dados e a importância de regulamentações mais claras e efetivas para proteger a privacidade e os direitos dos usuários na era digital.

1. CONTORNOS DA DEEP WEB

A "deep web" é um conceito tão antigo quanto a própria internet, referindo-se a um espaço virtual projetado para compartilhar informações sem restrições de filtros, governos ou intervenções políticas. Apesar de muitos associarem equivocadamente a "deep web" a atividades ilícitas, ela é fundamentalmente destinada a divulgar informações.

A "dark web", por outro lado, é mais conhecida internacionalmente e frequentemente ligada a atividades criminosas, mas também oferece recursos valiosos para aprendizado e uma visão menos limitada do mundo. Na "deep web", a liberdade humana é expressa em sua amplitude, livre de restrições impostas pelos meios de comunicação e governos, o que atrai um número crescente de adeptos para esse submundo virtual.

A compreensão da dinâmica de navegação na "deep web" é crucial para diferenciá-la da internet convencional, a "surface". Comparato explora a estrutura de poder e controle em empresas anônimas, aspecto associado à dinâmica da "deep web", onde identidades e ações dos usuários frequentemente permanecem ocultas.

Decisões e informações compartilhadas nesse espaço virtual podem impactar diretamente a privacidade e os direitos das partes envolvidas, refletindo no ciberespaço, onde a ausência de supervisão e regulamentação permite práticas que prejudicam a privacidade dos indivíduos.

Ao discutir aspectos éticos e legais, Comparato destaca a importância da transparência e divulgação de informações, princípios que podem ser aplicados no contexto da "deep web". Isso reforça a necessidade de considerar a privacidade como um valor fundamental ao tomar decisões e realizar atividades nesse ambiente virtual. A principal diferença entre a "deep web" e a "surface" está na ocultação dos números de identificação dos computadores, tornando extremamente difícil rastreá-los, facilitando a execução de atividades ilícitas por usuários mal-intencionados.

1.1 SERVIDOR HIBERNADO

Como explicado anteriormente, na internet comum, cada computador assume um número único quando ingressa no ambiente virtual, e diferentemente da internet comum, a *“deep web”* passa por uma série de criptografias que impossibilitam o rastreio do computador em si.

No mundo da internet, a comunicação entre os computadores não se dá de forma direta, mas sim através de diversos outros equipamentos. Nesse sentido, o conceito de

servidor, é um computador que contém as informações que necessitamos, e na internet comum, quando buscamos essa informação o sistema de DNS (Sistema de Domínio de Nomes) nos envia diretamente para o computador que possui essa informação. Basicamente o DNS, é um sistema de gerenciamento de nomes, onde contém registros com o nome do "*site* " e o número do IP à ele relacionado e quando o computador faz a busca, este é imediatamente direcionado para aquele número de equipamento especificado.

Na *"deep web"*, a requisição passa por diversos computadores, até possamos acessar a informação que necessitamos, de modo que não se sabe ao certo quem esta acessando aquele computador. Assim temos que o servidor encaminha todas as informações através da rede, e todos os computadores tem uma espécie de cópia do conteúdo acessado, em cada requisição, de forma, tudo que é acessado na internet tem cópias e mais cópias, no mundo virtual.

No entanto, na *"deep web"*, a criptografia permite que apenas os computadores requisitante e requisitado, possam decodificar a informação, de modo que, qualquer computador que intercepte as requisições, não conseguirá decifrar os dados.

Logo, temos que o servidor no ambiente virtual, trabalha de forma hibernada, ou seja, todas as informações que ele dispõe, não ficam arquivadas em memória virtual, mas sim, no disco rígido do próprio computador, ou seja, toda a informação que ele possui, encontra-se exclusivamente nele, não havendo cópias, o que impossibilita aos investigadores a interceptação de qualquer informação útil à localização do computador ou usuário. Neste sentido, a dificuldade de localização do servidor hibernado é extrema, o que, por sua vez, torna a procura de qualquer pista em relação aos crimes cometidos nesse ambiente, uma impossibilidade de proporções gigantescas.

Portanto, não havendo possibilidade de localização do computador que possibilita o cometimento de crimes, estes restam totalmente impunes, uma vez que o criminoso não pode ser localizado, para responder pelos seus atos ilícitos.

1.2 NAVEGAÇÃO NA "DEEP WEB"

O sistema da internet opera por meio de uma estrutura onde todas as informações são arquivadas por servidores e diversas outras ferramentas, visando controlar o fluxo de dados no meio virtual. Distinto da internet convencional, o submundo virtual opera em oposição à chamada "surface web". Nesse contexto, a "dark web" recebe um tratamento distinto, uma vez

que a transmissão de informações não está sujeita a qualquer tipo de controle governamental, institucional ou semelhante.

Enquanto na internet convencional todos os meios para registrar e supervisionar informações são empregados, na deep web, as informações circulam com uma liberdade completa, sem restrição de conteúdo. A ausência de controle estatal no ambiente virtual da "deep web" permite aos usuários transitarem sem restrições, o que facilita significativamente a ocorrência de variados crimes, independentemente de sua gravidade ou natureza.

A navegação nesse espaço virtual é complexa e lenta, já que não conta com o apoio financeiro de grandes corporações, estados ou organizações não governamentais que poderiam investir em infraestrutura para aprimorar seus servidores. Navegar nesse ambiente requer um conhecimento aprofundado em informática. Surpreendentemente, cerca de 90% dos usuários da internet convencional possuem pouca ou nenhuma compreensão sobre seu funcionamento, o que torna as informações valiosas e potencialmente perigosas para indivíduos mal-intencionados. É uma realidade incontestável que até mesmo os dados mais discretos podem ser explorados de modo criminoso por pessoas que almejam perpetrar fraudes e delitos no mundo virtual.

1.3 FUNCIONAMENTO "DEEP WEB"

Na "deep web", um sistema opera em que um computador solicita informações por meio da rede global de computadores. Essa requisição é processada em outro ponto, resultando em dados enviados de volta ao computador que fez a solicitação. A criptografia, um elemento-chave desse processo, pode ser comparada aos hieróglifos do antigo Egito, em que cada símbolo representava palavras, números ou objetos.

Na informática, a criptografia implica codificar informações em sequências de números ou letras, conhecidas como caracteres alfanuméricos. O computador de destino, detentor do código correspondente, decodifica as informações, processa-as e, após gerar o resultado, recodifica para retorná-lo ao computador de origem, assegurando a entrega segura de dados. Entretanto, na "deep web", onde a regulamentação é praticamente inexistente, a rastreabilidade das informações se torna uma tarefa desafiadora. Indivíduos versados em informática, compreendendo a complexidade da criptografia, aproveitam essa vantagem para perpetrar ações mais sofisticadas.

A criptografia pode ser explorada por pessoas mal-intencionadas que interceptam pacotes de dados e, após análise detalhada, iniciam o processo de decodificação. Para mitigar

essa ameaça, as técnicas de criptografia avançaram, ampliando os pacotes de dados para suportar mais substituições, tornando a decodificação uma tarefa altamente complexa, se não impossível. No ambiente da "deep web", hackers precisam adotar abordagens mais criativas para burlar a criptografia avançada utilizada por empresas.

Eles frequentemente lançam e-mails falsos com ofertas enganosas para atrair vítimas, levando-os a clicar em links que redirecionam para sites que implantam vírus, como cavalos de Troia, malwares e spywares. Quando infectados, os dados pessoais das vítimas podem ser roubados, resultando em desfalques financeiros, alterações de dados nas redes sociais e mudanças de senhas, entre outras consequências possíveis. Embora os crimes na internet convencional geralmente possam ser rastreados e punidos, na "deep web", a ausência de supervisão permite que criminosos operem com maior liberdade. Isso torna o ambiente propício para golpes, vírus e fraudes, dada a falta de restrições que facilitam essas atividades prejudiciais.

Em resumo, a criptografia na "deep web" é um desafio complexo, onde as informações podem ser interceptadas sem supervisão ou controle. Nesse ambiente virtual não regulamentado, o terreno fértil para atividades ilícitas exige que os usuários estejam bem informados para identificar e mitigar ameaças, evitando assim a propagação de golpes e fraudes.

2. LEI GERAL DE PROTEÇÃO DE DADOS E DEEP WEB

Num esforço notável, o legislador brasileiro, após diversas regulamentações sobre o uso da internet e violações aos direitos fundamentais de todos os indivíduos, modificou o Marco Civil da Internet, introduzindo uma nova legislação, a Lei Geral de Proteção de Dados Pessoais (LGPD). Esta atualização normativa reflete o compromisso com a proteção dos dados pessoais, estabelecendo diretrizes e regras para assegurar a privacidade e a segurança das informações dos cidadãos brasileiros. Essa iniciativa demonstra a busca por uma legislação mais abrangente e atualizada para lidar com os desafios e demandas da era digital.

Com a implementação dessa nova norma, sob uma perspectiva atualizada, a lei passou a apresentar uma lista específica do que considera como dados sensíveis dos usuários da internet no contexto brasileiro.

Além disso, estabeleceu uma postura mais rigorosa na fiscalização dos dados disponibilizados pelas plataformas, bem como definiu punições efetivas para possíveis abusos cometidos com as informações de seus usuários. Essa legislação busca não apenas definir

claramente os tipos de dados sensíveis, mas também promover um ambiente mais seguro e responsável no tratamento das informações pessoais dos usuários online. Nesse contexto, o rol detalhado pode ser identificado no artigo 5º dessa legislação, onde são estabelecidas as definições de dados pessoais, dados sensíveis, dados anonimizados, banco de dados, controlador, operador, tratamento e uma série de outros elementos. Esse rol compreende 19 itens abordados pela lei, cada um definindo e delimitando aspectos específicos relacionados ao tratamento e uso de dados pessoais, fornecendo um arcabouço detalhado para orientar as práticas e diretrizes no âmbito da proteção de dados.

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019) Vigência
> IX - agentes de tratamento: o controlador e o operador;
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
> XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
> XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
> XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
> XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

> XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
> XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
> XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e (Redação dada pela Lei nº 13.853, de 2019) Vigência
> XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (Redação dada pela Lei nº 13.853, de 2019) Vigência

A lei geral de proteção de dados desempenha um papel crucial ao antecipar e definir as terminologias atualmente empregadas para caracterizar o conceito de dados sensíveis. Em um momento subsequente dessa norma, ela detalha a aplicação apropriada dessas terminologias em ambientes digitais, bem como estabelece diretrizes para a fiscalização e utilização desses dados.

Contudo, essa abordagem pode, por vezes, inadvertidamente, fomentar uma coleta indiscriminada de dados, especialmente quando há imposições associadas ao consentimento de cookies e outros termos para acessar sítios eletrônicos.

Embora a legislação busque regulamentar e proteger a privacidade dos usuários, a necessidade de aceitar termos para a utilização de sites pode criar um cenário onde a concessão de consentimento se torna quase que uma exigência para o acesso digital. Isso pode influenciar a percepção do usuário sobre a segurança de seus dados, resultando em uma possível coleta excessiva de informações, mesmo quando o usuário não tem plena consciência ou controle sobre o que está sendo compartilhado.

Essa dualidade entre a proteção de dados e a praticidade na utilização de serviços online representa um desafio para a aplicação eficaz da legislação. É fundamental encontrar um equilíbrio que garanta a proteção dos dados pessoais dos usuários, ao mesmo tempo em que permita uma experiência digital fluida e transparente, sem sobrecarregar os usuários com solicitações excessivas de consentimento para o acesso aos serviços online.

Assim, é imprescindível a observância cautelosa e a fiscalização mais rigorosa dos sítios eletrônicos que impõem unilateralmente a aceitação de regras, as quais, por vezes, podem prejudicar os usuários.

É crucial encontrar um equilíbrio entre a conveniência na utilização desses serviços online e a proteção dos dados pessoais, garantindo que os termos e condições sejam transparentes e equitativos para os usuários. A aplicação criteriosa da legislação nesse sentido é fundamental para assegurar a proteção dos direitos individuais dos usuários enquanto se beneficia dos serviços oferecidos no ambiente digital.

PRINCIPAIS INFORMAÇÕES NOS VAZAMENTOS

Os vazamentos de dados na Deep web priorizam informações pessoais variadas, desde as mais básicas até aquelas mais complexas e detalhadas. Essas informações abrangem dados como nome, CPF, data de nascimento, nomes dos pais, estado civil, número de telefone, endereço residencial, escolaridade, histórico de emprego, renda, classe social, posse de benefícios, número de RG, informações fiscais como declaração de imposto de renda, mosaic (perfil demográfico), afinidades e até mesmo dados de óbito, todos com um alto nível de precisão.

Esses vazamentos representam uma grave ameaça à privacidade e à segurança das pessoas, pois expõem uma gama extremamente detalhada de informações pessoais, fornecendo uma visão abrangente da vida e do perfil de um indivíduo.

A precisão e a quantidade de dados disponíveis podem ser utilizadas para atividades maliciosas, como fraudes, roubos de identidade, espionagem e outros crimes cibernéticos. É crucial compreender a sensibilidade desses dados e adotar medidas rigorosas para proteger as informações pessoais, evitando assim potenciais violações e danos à privacidade dos indivíduos.

A empresa Tecnoblog, em conjunto com a DataBreaches.net, (VENTURA, 2022) trouxe em reportagem junto ao seu sítio eletrônico um rol de detalhes sobre o conjunto de vazamentos de dados na Deep Web:

- ✓ Básico: nome, CPF, gênero, data de nascimento, nome do pai, nome da mãe
- ✓ Estado civil (casado, solteiro, divorciado, viúvo, outros)
- ✓ Vínculo familiar: categoriza pessoas de acordo com vínculo de 1º grau (mãe, pai, filho, filha, irmão, irmã, cônjuge) ou 2º grau (avô, neto, tio, sobrinho, primo etc.)
- ✓ E-mail, Telefone, Endereço, Domicílios, Escolaridade;

- ✓ Universitários, Ocupação, Emprego, Salário, Renda, Classe social;
- ✓ Poder aquisitivo: nível (baixo, médio, alto), renda, salário
- ✓ Bolsa Família, Título de eleitor;
- ✓ RG, FGTS: número do PIS, CNS (Cartão Nacional de Saúde);
- ✓ NIS (Número de Identificação Social), PIS/PASEP, INSS, IRPF;
- ✓ Receita Federal, Score de crédito, Devedores, Cheques sem fundos;
- ✓ Mosaic, Afinidade, Modelo analítico, Fotos de rostos;
- ✓ Linkedin, Empresarial, Servidores públicos, Conselhos;
- ✓ Óbitos.

Nesse contexto, as empresas que se utilizam desses dados para conduzir campanhas e outras atividades, seja de forma legal ou ilícita, como nos casos de crimes cometidos na internet, têm uma considerável capacidade de atuação no ambiente digital, munidas de uma quantidade avassaladora de informações sobre seus clientes e/ou vítimas.

Esse acesso amplo a dados pessoais cria uma situação em que essas entidades podem ter um conhecimento detalhado e extenso dos perfis das pessoas, permitindo um direcionamento específico em suas estratégias, sejam elas comerciais ou criminosas, o que destaca a necessidade urgente de regulamentações mais rígidas para proteger a privacidade e a segurança dos indivíduos online.

PRINCIPAIS CASOS DE VAZAMENTOS DE DADOS DA HISTÓRIA

Os vazamentos de dados, tanto na internet convencional quanto na Deep web, foram uma das motivações para a instituição do Dia Internacional da Privacidade de Dados, celebrado em 28 de janeiro. Essa data reforçou a relevância da proteção da privacidade como um direito fundamental de liberdade no contexto do uso de dados pessoais.

A criação desse dia serve como um lembrete crucial sobre a importância de salvaguardar informações pessoais e reforçar medidas para proteger os dados dos usuários, diante dos desafios crescentes relacionados à privacidade e à segurança online. Apesar da existência do Regulamento Geral sobre a Proteção de Dados (GDPR) na Europa e da Lei Geral de Proteção de Dados (LGPD) no Brasil, ainda ocorrem abusos por parte de empresas no manejo de informações de clientes e usuários. Isso se manifesta na coleta de dados sensíveis e altamente pessoais, bem como no armazenamento dessas informações em servidores suscetíveis a vulnerabilidades, resultando em vazamentos, vendas e até mesmo trocas desses dados com outras entidades comerciais.

Essas práticas questionáveis ressaltam a necessidade de uma fiscalização mais rigorosa e de medidas efetivas para garantir a segurança e a privacidade dos dados dos indivíduos, visando coibir esses abusos e promover um tratamento responsável das

informações pessoais. Nesse contexto, o Núcleo de Direito Digital de Lara Martins compilou em seus estudos os 28 principais casos de vazamento de dados, abrangendo tanto incidentes de pequeno, médio quanto grande porte. Essa compilação destaca a relevância da proteção e armazenamento adequado dessas informações sensíveis. O levantamento desses casos emblemáticos serve como um alerta para a importância da segurança dos dados em todas as escalas, desde empresas menores até organizações de maior porte, evidenciando a necessidade de práticas eficazes de proteção de dados para evitar futuros vazamentos e preservar a privacidade dos indivíduos.

1 – Carolina Dieckmann – Em maio de 2011, um hacker (criminoso virtual) invadiu o computador pessoal da atriz, possibilitando que ele tivesse acesso a 36 fotos pessoais de cunho íntimo. De acordo com a denúncia, o invasor exigiu R$ 10 mil para não publicar as fotos. Como a atriz recusou a exigência, acabou tendo suas fotos divulgadas na internet. Isso criou uma grande discussão popular sobre a criminalização desse tipo de prática, que ainda foi excessivamente fomentada pela mídia. A atriz abraçou a causa e cedeu seu nome à Lei nº 12.737/2012.
2 – LinkedIn – Em junho de 2012, a rede social LinkedIn sofreu uma invasão que expôs os dados pessoais de mais de 117 milhões de usuários.
3 – Evernote – Em março de 2013, os sistemas do aplicativo de texto Evernote sofreu uma invasão que resultou do acesso não-autorizado a nomes de usuários, endereços de e-mail e senhas associadas às contas dos usuários da plataforma da empresa.
4 – Yahoo – Em agosto de 2013, após sofrer uma invasão, o site Yahoo informou o vazamento de dados como nome, telefone, data de nascimento e senha de 3 bilhões de usuários.
5 – Facebook/Cambridge Analytica – Em 2014, a Cambridge Analytica valeu-se de informações básicas (nome, profissão, cidade) e de hábitos e preferências políticas de 50 milhões usuários do Facebook para a realização não autorizada de testes comportamentais, que futuramente foram utilizados na campanha presidencial do ex-presidente do EUA, Donald Trump, e na votação do Brexit.
6 – eBay – Em maio de 2014, um vazamento de dados expôs as contas de 145 milhões de usuários (nomes, endereços, datas de nascimento e senhas criptografadas) da eBay, uma das maiores empresas de comércio eletrônico do mundo.
7 – Departamento de Imigração da Austrália – Em novembro de 2014, os dados pessoais dos líderes dos países que compõem o G20, tais como Barack Obama (EUA), Vladimir Putin (Russia), Angela Merkel (Alemanha) e Xi Jinping (China), foram expostos a partir de um acidente que ocorreu no Departamento de Imigração australiano.
8 – British Airways – Em março de 2015, os dados pessoais de milhares de passageiros da companhia aérea britânica British Airways foram acessados sem autorização, após uma invasão ao banco de dados de passageiros da empresa.
9 – Uber – Em 2016, o aplicativo de transporte Uber foi vítima de uma invasão que resultou no roubo de dados de mais de 57 milhões de usuários, incluindo 200 mil brasileiros. Esse caso de vazamento de dados, no entanto,

só veio a público em 2017 e a empresa foi multada em US$ 150 milhões pelo governo do estado da Califórnia, nos Estados Unidos.
10 – MySpace – Em maio de 2016, os usuários da rede social MySpace foram notificados que seus dados pessoais poderiam ter sido expostos e estar à venda online. Posteriormente, a Time Inc., empresa controladora da rede social, informou que o vazamento ocorreu em 2013 e afetou um total de 360 milhões de usuários.
11 – FriendFinder Network – Em novembro de 2016, os usuários da rede social de namoro FriendFinder Network tiveram seus dados pessoais acessados indevidamente por causa de mecanismos de segurança vulneráveis.
12 – Aeroporto de Heathrow (Reino Unido) – Em outubro de 2017, um pendrive foi perdido nas ruas de Londres contendo desde as medidas de segurança tomadas pela equipe da rainha da Inglaterra, bem como os números de identidade dos funcionários que acessam as áreas restritas de um dos maiores aeroportos do mundo.
13 – Netshoes – Em janeiro de 2018, o Ministério Público (MP) constatou que um incidente de segurança comprometeu dados pessoais como nome, CPF, e-mail, data de nascimento e histórico de compras de clientes da empresa Netshoes. Em acordo assinado com o MP, o site de comércio eletrônico pagou R$ 500 mil de indenização por danos morais.
14 – MyFitnessPal – Em fevereiro de 2018, 150 milhões de usuários do aplicativo MyFitnessPal tiveram seus usuários e endereços de e-mail vazados. Posteriormente, foi descoberto que o vazamento ocorreu em razão do uso de mecanismos de segurança que historicamente já haviam sido explorados para o acesso não autorizado aos dados dos usuários da rede social de namoro FriendFinder Network.
15 – C&A – Em 2018, a C&A, uma das maiores redes varejistas do Brasil, teve cerca de 2 milhões de dados de clientes cadastrados no sistema de vales-presente e trocas de suas lojas vazarem depois de um ciberataque realizado por hackers.
16 – Banco Inter – Em 2018, o Banco Inter, um dos pioneiros em oferecer contas digitais no país, registrou um vazamento que deixou vulnerável cerca de 19 mil correntistas. O vazamento dos dados aconteceu em uma ação que envolveu o envio, por um suposto hacker, de um arquivo criptografado que teria como conteúdo senhas, códigos de verificação, cheques, declarações de imposto de renda e dados pessoais dos clientes do banco. Em dezembro do mesmo ano, a empresa fechou um acordo com o Ministério Público e pagou uma multa de R$ 1 milhão, que foi destinada a instituições públicas de caridade e a organizações que trabalham combatendo o crime cibernético.
17 – Twitter – Em maio de 2018, solicitou que seus 330 milhões de usuários alterassem suas senhas após a descoberta de uma vulnerabilidade no banco de dados da rede social. Importante relembrar que anos antes, o mesmo Twitter entrou em acordo com a U.S. Federal Trade Commission, após a conclusão de que houve graves falhas de segurança que permitiram duas vezes o acesso aos dados pessoais dos usuários da rede social.
18 – Mariott – Em novembro de 2018, a rede hoteleira Mariott sofreu o vazamento de 500 milhões de dados pessoais de hóspedes. O acesso não autorizado aos dados, entretanto, ocorria desde 2014, a partir do banco de dados da rede de hotéis Starwood, adquirida pelo Mariott em 2016.
19 – Detran-RN – Uma falha de segurança no site do Departamento de Trânsito do Rio Grande do Norte (Detran-RN) provocou o vazamento de dados de mais 70 milhões de motoristas em todo o país. O fato aconteceu em 2019 e, à época, todos os brasileiros que tinham CNH foram afetados, já que os Detrans possuem sistemas integrados.

20 – McDonald’s – Em outubro de 2019, mais de 2 milhões de registros sensíveis da rede McDonald’s Brasil vazaram e foi possível acessar dados pessoais como nome completo, faixa etária, tempo de experiência, cargo, seção, etnia, necessidades especiais, salário e até mesmo unidade de trabalho dos funcionários. O vazamento permitiu ainda acessar 76 mil registros de novas contratações, 12 mil fichas de demissão e uma lista com 245 fornecedores e parceiros, com dados como nome da empresa, e-mail de contato e CNPJ.
21 – Ministério da Saúde – No final de 2020, o vazamento da base cadastral do Ministério da Saúde expôs os dados de 243 milhões de cidadãos na Internet. O número, acima da população brasileira atual — estimada em 213,3 milhões de habitantes, segundo o IBGE —, é explicado pelo fato de haver também dados de pessoas já falecidas.
22 – Brasil – Em janeiro de 2021, arquivos com dados pessoais de mais de 223 milhões de brasileiros apareceram em fóruns usados por criminosos digitais. Os dados eram separados por número de CPF e também estão acompanhados de informações de veículos cadastrados no Brasil. Um ano depois, o episódio, que ficou conhecido como megavazamento de dados ainda é investigado pela Autoridade Nacional de Proteção de Dados (ANPD) e sua origem é desconhecida.
23 – Brasil – Menos de um mês após o megavazamento de dados, de janeiro de 2021, a empresa de cibersegurança Psafe descobriu outro banco de dados à venda na dark web com mais de 100 milhões de celulares brasileiros. Além do número do telefone, a base continha nome completo, endereço e CPF do assinante da linha. Até o momento a sua origem é desconhecida.
24 – Amazon – Em julho de 2021, a empresa recebeu a multa de € 746 milhões da Comissão Nacional de Proteção de Dados de Luxemburgo em razão da não conformidade aos princípios da proteção de dados do seu sistema de publicidade direcionada. Até o momento é a maior multa imposta desde a entrada em vigor do Regulamento Geral sobre a Proteção de Dados (GDPR), na Europa.
25 – Lojas Renner – Em agosto de 2021, a rede Lojas Renner sofreu um ataque cibernético. O ataque resultou na inutilização temporária dos servidores da empresa, o que resultou na paralisação de parte das operações físicas e total das operações online.
26 – Banco do Estado de Sergipe – Em outubro de 2021, por meio da técnica de engenharia social, cerca de 395 mil chaves do sistema de pagamento instantâneo PIX que estavam sob a tutela do Banco do Estado de Sergipe (Banese) foram obtidas por hackers. Em nota, o Banco Central afirma que não foram expostos dados sensíveis, como senhas, valores movimentados e saldos nas contas. Ainda de acordo com o informativo, as chaves vazadas não são de clientes do banco, e que o acesso indevido aconteceu por conta de “falhas pontuais” no sistema do Banese.
27 – Twitch/Amazon – Em outubro de 2021, a Twitch, plataforma de streaming da Amazon, sofreu um vazamento de dados pessoais ocasionada por um erro de configuração dos servidores. Aproximadamente 125 GB de dados foram vazados, dentre os quais estão os pagamentos recebidos pelos streamers da plataforma nos últimos 2 anos.
28 – Facebook – Em outubro de 2021, os servidores da empresa responsável pelas redes sociais Facebook, Instagram e aplicativo de mensagens WhatsApp ficaram 6 horas fora ar por causa de um erro de configuração nos servidores, o que impediu cerca de 3.5 bilhões de usuários de acessarem as plataformas da empresa e suas informações pessoais.

Essas informações ressaltam a importância singular de as pessoas desfrutarem de segurança ao fornecer informações em plataformas digitais, onde podem, inadvertidamente, figurar como vítimas ou protagonistas em vazamentos de dados, sejam esses intencionais ou não.

Destacar essa questão reforça a necessidade de promover uma cultura de proteção de dados que não apenas garanta a segurança dos usuários, mas também os capacite a tomar decisões informadas sobre o compartilhamento de informações online.

É crucial desenvolver medidas proativas para mitigar os riscos de vazamento de dados, considerando tanto a responsabilidade das plataformas quanto a conscientização e a proteção dos indivíduos diante dessas situações.

DEEP WEB E LGPD

Em 2021, o cenário nacional ficou estarrecido de que 223 milhões de CPFS, destes quais incluindo-se ou de pessoas falecidas além de 40 milhões de CNPJ e 104 milhões de registro de veículos haviam sido vazados junto a Deep Web e esses dados poderiam ser utilizados com as mais diversas finalidades, uma vez que, em relação aos CPF, havia outras informações como nome completo, data de nascimento, fotos de rosto, escola de crédito, renda, dado de Imposto de Renda, telefone, escolaridade, benefício entre outras informações e em relação aos veículos, era possível encontrar chassi, placa, município, cor, marca, modelo, ano de fabricação e até mesmo o tipo de combustível utilizado por eles.

A fonte do vazamento foi devidamente investigada pela Polícia Federal, em determinação dada pelo Supremo Tribunal Federal, antes mesmo da efetivação da ANPD, Agência Nacional de Proteção de Dados, Para que houvesse um efetivo resultado quando da exposição de praticamente todos os brasileiros a ação de criminosos.

Uma das maiores informações vazadas Deuses pelo Serasa Experian, através do mosaic, que trazem informações relevantes sobre as condições financeiras de todos os brasileiros referentes a renda e também possíveis restrições, o que traria uma possibilidade de análise aprofundada sobre quais vítimas poderiam estar sendo utilizadas em ações criminosas.

Ainda, houve outro vazamento em relação ao Facebook que teve cerca de 553 milhões de usuários expostos quando da ação criminosa de hackers que divulgaram foram número de telefone, nome completo, localização, data de nascimento, login da rede social e, em alguns casos, endereço de e-mail.

Esses dados, são em geral comercializados ilegalmente através da deep web podendo ser utilizados para prática de crimes contra os titulares dos dados ou de empresas Ou ainda fornecidos para outras empresas que buscam um resultado efetivo em suas campanhas e/ou plataformas.

Com isso, houve diversas tentativas do governo nacional em trazer uma regulamentação junto ao âmbito da internet culminando com a edição da lei geral de proteção de dados, em 2020, para figurar como forte aliada na proteção de dados contra ações criminosas diversas.

Nesse sentido, a lei geral de proteção de dados, tornou-se uma aliada importante na proteção de crédito e prevenção de fraudes pois determinou a introdução de novas ferramentas para a obtenção de crédito, ferramentas essas como identificação facial, ações de informações bancárias entre outras que pudessem efetivamente ludibriar a ação de criminosos no âmbito virtual.

Destaca-se que a LGPD é uma aliada da proteção ao crédito e da prevenção à fraude, pois permite o tratamento de dados pessoais e sensíveis com as referidas finalidades, independentemente do consentimento do titular. Assim, as empresas que comercializam produtos e serviços pela internet podem utilizar-se de diversos recursos disponíveis no mercado para coibir fraudes.

É crucial ressaltar que a Lei Geral de Proteção de Dados (LGPD) interage com outras regulamentações, conferindo maior confiabilidade aos usuários de sistemas de crédito e diversas plataformas digitais. Em primeiro lugar, destaca-se a Lei do Cadastro Positivo, cuja função primordial é construir um histórico de crédito tanto para pessoas físicas quanto jurídicas.

Além disso, a Lei de Lavagem de Dinheiro estabeleceu a implementação do "Conheça Seu Cliente" (Know Your Client - KYC), exigindo uma identificação eficaz para cadastrar-se nas plataformas, assegurando a legitimidade do usuário.

Esta interação entre normas visa aprimorar a confiança e transparência no uso dos dados, promovendo um ambiente mais seguro e confiável para os indivíduos e organizações.

Ao final, a empresa realizará uma análise jurídica apropriada das operações realizadas, juntamente com as medidas tomadas para salvaguardar o crédito. Isso permitirá que o tratamento de dados pessoais e sensíveis esteja em conformidade com os direitos dos titulares em duas vertentes distintas.

Ao embasar o processamento desses dados na LGPD e em leis pertinentes, em prevenir o uso indevido por terceiros, protegendo os dados pessoais e evitando potenciais crimes que possam afetar tanto os titulares quanto a empresa em questão.

CONCLUSÃO

No contexto da deep web, compreender a extensão e a aplicabilidade da LGPD torna-se crucial quando se identificam os responsáveis pelo vazamento de informações, sejam elas sensíveis ou não, dos usuários da internet.

Essa identificação pode ocorrer por meio de contratos estabelecidos entre empresas ou por ações de hackers que invadem sistemas, copiam dados e os disponibilizam em sites que buscam essas informações para embasar suas atividades.

A LGPD, nesses casos, desempenha um papel fundamental ao delinear as responsabilidades e penalidades para indivíduos ou entidades envolvidas na obtenção e uso indevido de dados, independentemente de estarem na *deep web* ou em qualquer outro ambiente da internet.

Sua aplicação não se restringe apenas à superfície visível da rede, mas estende-se aos recônditos mais ocultos, buscando salvaguardar os direitos dos titulares dos dados e assegurar que a privacidade e segurança sejam preservadas, independentemente do contexto em que os dados circulem ou sejam explorados.

Na aplicação da LGPD em tais circunstâncias, é relevante ressaltar que os responsáveis, identificados por meio de contratos estabelecidos entre as partes, podem ser integralmente responsabilizados, uma vez que suas ações demonstram um nível de transparência que viabiliza a investigação e, consequentemente, a aplicação das disposições da norma.

A existência de acordos contratuais claros e transparentes oferece uma base sólida para a verificação de conformidade com a LGPD, permitindo uma compreensão clara das responsabilidades atribuídas a cada parte envolvida. Essa transparência nas operações estabelece uma fundação robusta para a verificação de conformidade com as diretrizes da LGPD, possibilitando uma avaliação detalhada das práticas adotadas e garantindo que as medidas corretivas ou sancionatórias sejam aplicadas, caso necessário, de acordo com os parâmetros legais estabelecidos pela norma.

Assim, a clareza nos contratos entre as partes facilita a fiscalização e a garantia da conformidade com os princípios e diretrizes estipulados pela LGPD, promovendo a proteção efetiva dos dados e dos direitos dos titulares.

No contexto dos ataques hackers, é essencial destacar que, na maioria das situações, a identificação desses indivíduos se torna extremamente desafiadora devido ao uso de diversos artifícios para ocultar suas verdadeiras identidades.

Esse cenário dificulta significativamente a atuação dos órgãos de fiscalização e das autoridades policiais, que enfrentam obstáculos consideráveis para punir os crimes cometidos nesse âmbito. A habilidade dos hackers em utilizar diferentes métodos para camuflar suas pegadas digitais e ocultar-se por trás de várias camadas de anonimato resulta em uma investigação complexa e muitas vezes infrutífera.

Tal dificuldade torna-se um desafio para os órgãos responsáveis pela aplicação da lei, pois a falta de informações concretas sobre a identidade dos criminosos cibernéticos limita suas ações e compromete a eficácia na repressão desses delitos. É crucial desenvolver estratégias avançadas de segurança cibernética e colaboração internacional entre agências para minimizar essas lacunas de identificação e garantir uma resposta mais eficiente diante dos ataques perpetrados por hackers.

Portanto, a aplicação da LGPD no contexto da *deep web* enfrenta um desafio central: a identificação precisa do responsável pelo vazamento de informações, muitas vezes não ocorre prontamente. Isso exige uma série extensa de investigações para esclarecer os fatos.

Somente após a realização de todas as diligências necessárias e, se bem-sucedidas, é possível proceder com as devidas penalidades, seja criminal, indenizatória ou administrativa, em relação aos vazamentos. Isso pode incluir a adoção de ferramentas específicas que proporcionem maior segurança aos usuários das plataformas, visando prevenir futuros incidentes.

A complexidade da deep web, onde a identidade dos agentes pode estar oculta, demanda uma abordagem meticulosa para coletar evidências suficientes que possam levar à identificação dos responsáveis pelos vazamentos. Esse processo prolongado de investigação pode resultar em obstáculos significativos para os órgãos reguladores e autoridades competentes, dificultando a aplicação efetiva da legislação de proteção de dados.

Assim, a implementação da LGPD nesses casos requer não apenas medidas reativas, mas também estratégias preventivas, como o uso de tecnologias mais seguras e robustas, a fim de mitigar riscos e proteger a privacidade dos usuários.

É fundamental adotar abordagens multidisciplinares que combinem aspectos legais, técnicos e de segurança da informação para fortalecer a aplicação da LGPD na deep web, visando garantir a proteção dos dados e a responsabilização dos envolvidos em eventuais violações.

REFERÊNCIAIS BIBLIOGRÁFICAS

ALCÂNTARA, L. M. de. **Ciberativismo e movimentos sociais: mapeando discussões**. Aurora., v. 8, n. 23, p. 73-97, 2015. ISSN 1982-6672. Disponível em: Disponível em: https://revistas.pucsp.br/index.php/aurora/article/view/ 22474 Acesso em: 13 nov. 2023.

ARAUJO, Tiago. Veirano Advogados. **Vazamento de dados aumentaram 493% no Brasil, segundo pesquisa do MIT.** Atualizado em 24 fev 2021, 16h06 - Publicado em 24 fev 2021, 16h00. Disponível em: https://vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit. Acessado em 09/12/2023.

BRASIL. **Constituição Federal**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 29 de ago. de 2023.

BRASIL. **Lei 12.735/**2012. Disponível em: <http://www.planalto.gov.br/cciv il_03/_ato2011-2014/2012/lei/l12735.htm>. Acesso em 29 de ago. de 2023.

BRASIL. **Lei 12.737/2012**. Disponível em: <http://www.planalto.gov.br/cci vil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em 29 de ago. de 2023.

BRASIL. **Lei de Introdução do Código Penal**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del3914.htm>. Acesso em 29 de ago. de 2023.

BRASIL. **Lei Geral de Proteção de Dados.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 29 de ago. de 2023.

BRASIL. **Lei 12.965/2014**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 29 de ago. de 2023.

BRASIL. **Ministério da Educação. Base Nacional Comum Curricular**. [S.l.: s.n.], 2018.

CASTELLS, Manuel. A Revolução da Tecnologia da Informação. in: CASTELLS, Manuel**. Sociedade em Rede.** Trad. Roneide Vecancio Majer. 22ª ed. São Paulo: Paz e Terra, , p. 87-133, 2020.

COHEN, Julie E. **Configuring the Networked Self: Law, Code, and the Play of Everyday Practice.** Yale University Press, 1ª ed, 2012.

COMPARATO, Fábio. **O poder de controle na sociedade anônima**. São Paulo : Revista dos Tribunais, 1976.

COSTA JR, P.J. **O direito de estar só – tutela penal da intimidade** – 4ª ed. rev. e atual. São Paulo: Editora Revista dos Tribunais, 2007.

DINIZ, M.H. **Teoria Geral do Direito Civil, 1º volume**, Editora Saraiva, 22ª ed. 2005. São Paulo.

JÚNIOR, TÉRCIO SAMPAIO FERRAZ, **Sigilo De Dados: O Direito à Privacidade e Os Limites À Função Fiscalizadora do Estado.** Revista da Faculdade de Direito, Universidade de São Paulo. São Paulo. 1993.

KULA, Emerson Luiz,. 18/08/2023 . IT Project Manager | MBA | PSM | Hybrid Projects.**Seus dados vazados na Deep Web?**.https://www.linkedin.com/pulse/seus-dados-vazados-na-deep-web-emerson-luiz-kula/?originalSubdomain=pt. Acessado em 09/12/2023.

LANKSHEAR, C.; KNOBEL, M. (Ed.). **Digital literacies: concepts, policies and practices.** New York: Peter Lang, 2008.

LÉVY, Pierre. **Cibercultura**. 1ª ed. Trad. Carlos Irineu da Costa. São Paulo. Editora 34, 1999.

RAYMOND, E.S. **The New hacker's dictionary**. MIT Press. .ISBN 0-262-68092-0 5ª ed, 1991.

ROHR, Altieres.28/01/2021.**Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber**.https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml. Acessado em 09/12/2023.

SOLOVE, Daniel, **Understanding Privacy**, Harvard University Press, 2ª ed, 2008.

SCHÖNBERGER, Viktor Mayer-, **Delete: The Virtue of Forgetting in the Digital Age,** Princeton University Press, 1ª ed, 2009.

VENTURA, Felipe.. **Exclusivo: vazamento que expôs 220 milhões de brasileiros é pior do que se pensava.** Disponível em: https://tecnoblog.net/noticias/2021/01/22/exclusivo-vazamento-que-expos-220-milhoes-de-brasileiros-e-pior-do-que-se-pensava/. Acessado em 09/12/2023.