

I ENCONTRO NACIONAL DE DIREITO DO FUTURO

**DIREITO DIGITAL, ALGORITMOS, VIGILÂNCIA E
DESINFORMAÇÃO III**

D598

Direito Digital, algoritmos, vigilância e desinformação III [Recurso eletrônico on-line]
organização I Encontro Nacional de Direito do Futuro: Escola Superior Dom Helder Câmara –
Belo Horizonte;

Coordenadores: Karina da Hora Farias, Wilson de Freitas Monteiro e Meire Aparecida
Furbino Marques – Belo Horizonte: Escola Superior Dom Helder Câmara - ESDHC, 2024.

Inclui bibliografia

ISBN: 978-85-5505-946-9

Modo de acesso: www.conpedi.org.br em publicações

Tema: Os desafios do humanismo na era digital.

1. Direito do Futuro. 2. Humanismo. 3. Era digital. I. I Encontro Nacional de Direito do
Futuro (1:2024 : Belo Horizonte, MG).

CDU: 34



I ENCONTRO NACIONAL DE DIREITO DO FUTURO

DIREITO DIGITAL, ALGORITMOS, VIGILÂNCIA E DESINFORMAÇÃO III

Apresentação

O Encontro Nacional de Direito do Futuro, realizado nos dias 20 e 21 de junho de 2024 em formato híbrido, constitui-se, já em sua primeira edição, como um dos maiores eventos científicos de Direito do Brasil. O evento gerou números impressionantes: 374 pesquisas aprovadas, que foram produzidas por 502 pesquisadores. Além do Distrito Federal, 19 estados da federação brasileira estiveram representados, quais sejam, Amazonas, Amapá, Bahia, Ceará, Goiás, Maranhão, Minas Gerais, Mato Grosso do Sul, Paraíba, Pernambuco, Paraná, Rio de Janeiro, Rio Grande do Norte, Rondônia, Rio Grande do Sul, Santa Catarina, Sergipe, São Paulo e Tocantins.

A condução dos 29 grupos de trabalho do evento, que geraram uma coletânea de igual número de livros que ora são apresentados à comunidade científica nacional, contou com a valiosa colaboração de 69 professoras e professores universitários de todo o país. Esses livros são compostos pelos trabalhos que passaram pelo rigoroso processo double blind peer review (avaliação cega por pares) dentro da plataforma CONPEDI. A coletânea contém o que há de mais recente e relevante em termos de discussão acadêmica sobre as perspectivas dos principais ramos do Direito.

Tamanho sucesso não seria possível sem o apoio institucional de entidades como o Conselho Nacional de Pesquisa e Pós-graduação em Direito (CONPEDI), a Universidade do Estado do Amazonas (UEA), o Mestrado Profissional em Direito e Inovação da Universidade Católica de Pernambuco (PPGDI/UNICAP), o Programa RECAJ-UFGM – Ensino, Pesquisa e Extensão em Acesso à Justiça e Solução de Conflitos da Faculdade de Direito da Universidade Federal de Minas Gerais, a Comissão de Direito e Inteligência Artificial da Ordem dos Advogados do Brasil – Seção Minas Gerais, o Grupo de Pesquisa em Direito, Políticas Públicas e Tecnologia Digital da Faculdade de Direito de Franca e as entidades estudantis da UFGM: o Centro Acadêmico Afonso Pena (CAAP) e o Centro Acadêmico de Ciências do Estado (CACE).

Os painéis temáticos do congresso contaram com a presença de renomados especialistas do Direito nacional. A abertura foi realizada pelo professor Edgar Gastón Jacobs Flores Filho e pela professora Lorena Muniz de Castro e Lage, que discorreram sobre o tema “Educação jurídica do futuro”. O professor Caio Lara conduziu o debate. No segundo e derradeiro dia, no painel “O Judiciário e a Advocacia do futuro”, participaram o juiz Rodrigo Martins Faria,

os servidores do TJMG Priscila Sousa e Guilherme Chiodi, além da advogada e professora Camila Soares. O debate contou com a mediação da professora Helen Cristina de Almeida Silva. Houve, ainda, no encerramento, a emocionante apresentação da pesquisa intitulada “Construindo um ambiente de saúde acessível: abordagens para respeitar os direitos dos pacientes surdos no futuro”, que foi realizada pelo graduando Gabriel Otávio Rocha Benfica em Linguagem Brasileira de Sinais (LIBRAS). Ele foi auxiliado por seus intérpretes Beatriz Diniz e Daniel Nonato.

A coletânea produzida a partir do evento e que agora é tornada pública tem um inegável valor científico. Seu objetivo é contribuir para a ciência jurídica e promover o aprofundamento da relação entre graduação e pós-graduação, seguindo as diretrizes oficiais da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES). Além disso, busca-se formar novos pesquisadores nas mais diversas áreas do Direito, considerando a participação expressiva de estudantes de graduação nas atividades.

A Escola Superior Dom Helder Câmara, promotora desse evento que entra definitivamente no calendário científico nacional, é ligada à Rede Internacional de Educação dos Jesuítas, da Companhia de Jesus – Ordem Religiosa da Igreja Católica, fundada por Santo Inácio de Loyola em 1540. Atualmente, tal rede tem aproximadamente três milhões de estudantes, com 2.700 escolas, 850 colégios e 209 universidades presentes em todos os continentes. Mantida pela Fundação Movimento Direito e Cidadania e criada em 1998, a Dom Helder dá continuidade a uma prática ético-social, por meio de atividades de promoção humana, da defesa dos direitos fundamentais, da construção feliz e esperançosa de uma cultura da paz e da justiça.

A Dom Helder mantém um consolidado Programa de Pós-graduação Stricto Sensu em Direito Ambiental e Sustentabilidade, que é referência no país, com entradas nos níveis de mestrado, doutorado e pós-doutorado. Mantém revistas científicas, como a Veredas do Direito (Qualis A1), focada em Direito Ambiental, e a Dom Helder Revista de Direito, que recentemente recebeu o conceito Qualis A3.

Expressamos nossos agradecimentos a todos os pesquisadores por sua inestimável contribuição e desejamos a todos uma leitura excelente e proveitosa!

Belo Horizonte-MG, 29 de julho de 2024.

Prof. Dr. Paulo Umberto Stumpf – Reitor da ESDHC

Prof. Dr. Franclim Jorge Sobral de Brito – Vice-Reitor e Pró-Reitor de Graduação da ESDHC

Prof. Dr. Caio Augusto Souza Lara – Pró-Reitor de Pesquisa da ESDHC

UMA ANÁLISE DA EFICÁCIA DA LEI GERAL DE PROTEÇÃO DE DADOS NA SALVAGUARDA DE DADOS PESSOAIS NA DEEP WEB

AN ANALYSIS OF THE EFFECTIVENESS OF THE GENERAL DATA PROTECTION LAW IN SAFEGUARDING PERSONAL DATA ON THE DEEP WEB

**Amanda Melissa Rodrigues Hansen Ferreira
Marina França Santos**

Resumo

Este projeto analisa a eficácia da Lei Geral de Proteção de Dados (LGPD), lei que garante a segurança de dados pessoais, no que tange os vazamentos de dados na Deep Web, rede marcada pelo anonimato e alta criminalidade. A pesquisa focou na aplicação da LGPD, avaliando sua eficiência na proteção de dados em âmbitos virtuais, contendo uma revisão bibliográfica com artigos publicados entre 2019 e 2024. À luz da revisão, sugere-se que apesar das intenções da LGPD, a fiscalização efetiva e a responsabilização das empresas precisam ser reforçadas, enfatizando a insuficiência dessa lei na garantia da salvaguarda de dados pessoais.

Palavras-chave: Lgpd, Deep web, Cibercrime, Segurança

Abstract/Resumen/Résumé

This project analyzes the effectiveness of the General Data Protection Law (GDPL), a law that guarantees the security of personal data, against data leaks on the Deep Web, a network marked by anonymity and high criminality. The research focused on the application and effectiveness of the GDPL in data protection in virtual environments, containing a bibliographic review with articles published between 2019 and 2024. In light of the review, it is suggested that despite the GDPL's intentions, effective oversight and accountability of companies need to be strengthened, emphasizing the insufficiency of this law in guaranteeing the safeguarding of personal data.

Keywords/Palabras-claves/Mots-clés: Gdpl, Deep web, Cibercrime, Security

1. CONSIDERAÇÕES INICIAIS

O projeto de investigação científica em questão visa abordar a ocorrência dos frequentes vazamentos de dados em locais como a *Deep Web*, onde ao se cadastrar informações básicas em determinado site, o usuário corre um grande risco desses dados privados serem vazados. Por conta disso, torna-se necessária a existência de uma legislação que garanta a preservação e regulação de informações particulares, destacando-se a criação da Lei Geral de Proteção de Dados (LGPD), cujo objetivo é resguardar esses detalhes pessoais, intencionando maior segurança e privacidade para os consumidores. Portanto, tendo em vista que a internet é dividida em três camadas, sendo elas: a *Surface Web*, a *Deep Web* e a *Dark Web* (que é mais uma subclassificação da *Deep Web*), entende-se que esta pesquisa vislumbra toda a questão envolvendo os limites nos quais a eficácia da LGPD se encontra e até onde essa legislação consegue proteger seus usuários, levando em consideração todas as suas dificuldades e a sua possível aplicabilidade nas camadas supracitadas da internet.

O objetivo geral do presente trabalho é analisar a abrangência da Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018) no tocante à proteção e regulação dos dados pessoais de usuários no meio digital. Relacionando a funcionalidade e a eficácia dessa inovação não só na divisão disponível para acesso universal (apelada como *Surface Web*), mas também como e se ela atua em um ambiente pouco acessado e regulamentado como a *Deep Web* (frequentemente associada a atividades ilegais). Como objetivos específicos, enumeram-se os seguintes: 1) Análise da eficácia de aplicabilidade da LGPD em ambientes virtuais nas camadas da internet (*Surface Web*, *Deep Web* e *Dark Web*) ; 2) Descrever o papel da legislação vigente na proteção dos usuários, assim como apresentar uma investigação acerca do vazamento de dados e para que esses dados são utilizados ; 3) Abordar sobre questões envolvendo o uso da LGPD e a vulnerabilidade a que os usuários digitais são submetidos, trazendo também, ao contexto dos algoritmos e bancos de dados coletados através de sites diversos.

Ao se observar o contexto do surgimento de um grande volume de dados advindos da Globalização e da expansão da internet, visualiza-se que a proteção dos dados privados dos usuários passou a se tornar essencial, tendo em vista a extrema vulnerabilidade que esses indivíduos se encontram no ambiente virtual. Assim, fazendo com que a Lei Geral de Proteção de Dados entre em vigor visando proteger as informações privadas desses indivíduos, consequentemente tornando fundamental a análise da eficácia dessa legislação, especialmente

em ambientes que funcionam como dificultadores de fiscalizações como a *Deep Web*. Enfatizando a importância dessa análise no aumento de visibilidade da temática, gerando uma maior conscientização e destaque do tema para autoridades e serviços de inteligência.

Levando em consideração o anonimato frequentemente associado ao acesso da *Deep Web*, tem-se o fato de que a fiscalização e a atuação de legislações no meio virtual são dificultadas. Porém, pode-se apresentar como uma possível hipótese que a LGPD, levando em consideração que é uma lei específica para a proteção de dados, tem uma eficácia maior que outras legislações no que tange o resguardo das informações privadas dos usuários, inclusive em ambientes como a *Deep Web*.

Para o desenvolvimento dessa pesquisa, propõe-se uma revisão de literatura, em que os artigos serão selecionados por meio de uma busca na plataforma Google Acadêmico, utilizando como critério as palavras-chave. Os trabalhos que serão incluídos nesta análise deverão ter sido publicados entre os anos de 2019 a 2024, nos idiomas Português e/ou Inglês. Foram utilizados como critérios de exclusão artigos não disponíveis na íntegra e que não tenham relação direta com o objeto da pesquisa.

2. Cenário Legal Brasileiro e a Proteção de Dados

Consoante Barreto (2016), em meados da década de 1990, destaca-se uma potente revolução tecnológica e o surgimento de um ciberespaço no Brasil, bem como maior reconhecimento da internet globalmente, modificando a disponibilização do conhecimento e da informação. Diante disso, entende-se que, paralelamente ao uso frequente da internet, foi crescendo a existência de dados pessoais dos usuários e a necessidade de proteção e privacidade desses, haja vista a vulnerabilidade a que essas pessoas estão submetidas a partir do momento em que navegam na internet.

Com base nisso, é válido mencionar que, durante um extenso período, o cenário brasileiro relacionado às leis encontrava-se inadequado em decorrência da carência de leis que abrangesse a proteção de dados dos usuários, levando em consideração que não existiam legislações específicas que tangesse a salvaguarda desses dados (Such *et al.*, 2020). Visto isso, muitas vezes a conjuntura brasileira recorria à analogia para solucionar esses casos, isto é, partiam de premissas semelhantes para se chegar a uma conclusão ou até mesmo recorriam a

interpretações analógicas visando abranger esses casos que não eram amparados pelo sistema legal. Assim, tornou-se fundamental a criação de legislações específicas que resguardassem problemáticas envolvendo os dados dos usuários, a exemplo do surgimento do Marco Civil da internet e da Lei Geral de Proteção de Dados (LGPD).

Nesse contexto, identifica-se o Marco Civil da Internet, Lei 12.965/2014, como a Constituição da Internet que fundamenta a regulamentação do uso da Internet, tendo como inspiração os princípios já previstos na Constituição Federal, tais como o de liberdade de expressão (Killian, 2020). De maneira análoga, infere-se a criação da Lei Geral de Proteção de Dados (LGPD), a qual foi formulada justamente para promover o uso seguro dos dados pessoais dos indivíduos, tendo em vista que o Marco Civil da Internet era uma lei muito ampla e não apresentava a eficácia necessária no que diz respeito à proteção de dados, especialmente em decorrência da alta demanda exigida dessa legislação, de acordo com Mulholland (2020, *apud* Araújo; Cavalcanti; Souza, 2023). Desse modo, observa-se que foram criadas outras leis que regulamentam o ambiente virtual, a saber, a Lei Carolina Dieckmann, que criminaliza invasões de dispositivos informativos, contribuindo para maior fiscalização e penalização do âmbito virtual, que durante um bom tempo foi considerado como "livre" e "sem leis".

É importante fazer uma análise mais aprofundada da LGPD, Lei 13.709/2018, sendo necessário mencionar que, baseando-se em Silveira et al. (2016, *apud* Neves *et al.*, 2021), existem três tipos de dados que são encontrados na internet, sendo eles: os dados sensíveis (relacionados à personalidade e à vida pessoal do usuário), os dados identificáveis (abrange por exemplo o nº do cartão) e os dados identificados (que dizem respeito ao CPF, RG, etc). Visto isso, contempla-se que esses tipos de dados geralmente são utilizados por empresas e instituições, fazendo com que a LGPD objetive proteger esses dados armazenados pelas empresas para que eles sejam utilizados de forma regulamentada, evitando ocorrências de vazamentos de dados ou até mesmo manipulações. Assim, constata-se que esse marco legal, apesar de ser uma ferramenta muito recente, é considerado um mecanismo com potencial eficaz e de grande avanço para a proteção e fiscalização no mundo digital. Entretanto, no tocante à sua celeridade e execução prática, existem falhas e, por conseguinte, facilitação de operações criminosas no âmbito virtual, especialmente em decorrência dos anonimatos corriqueiros nesse ambiente.

3. Desafios da LGPD no que tange a violação de dados e o anonimato virtual

Ao considerar o anonimato no recinto virtual um desafio para a plena aplicação das legislações vigentes, compreende-se que existem outras maneiras que possibilitam o roubo desses dados, a exemplo dos meios trazidos por Siqueira *et al.* (2021), apelidados como malwares e vírus de computadores. Nesse contexto, segundo o autor, essas são as formas de violações digitais mais praticadas e onde tais crimes virtuais são mais perpetuados, exemplificados por meio do uso dessas ferramentas para acessar contas bancárias, fraudar cartões, usurpar bancos de dados de empresas, entre outros. À luz das informações expostas, percebe-se que essas transgressões digitais tornam-se cada vez mais frequentes no ambiente virtual, fazendo com que existam locais em que essa propagação criminosa seja muito mais frequente, podendo citar a *Deep Web* como um dos recintos que mais se destacam por sua atividade criminosa e anonimato.

Outrossim, é necessário estabelecer uma breve apresentação das camadas da internet fornecida de forma simplificada pelos autores Barreto e Santos (2019) em seu livro "*Deep Web: Investigação no submundo da internet*", no qual evidencia que a internet é composta por várias redes, sendo dividida em camadas: a *Surface Web*, a *Deep Web* e a *Dark Web*, sua subclassificação. A *Surface Web* é considerada o conjunto de páginas, sites e conteúdos que são utilizados diariamente pelas pessoas e empresas, contendo inúmeras informações, bancos de dados e páginas da web. Em sequência, tem-se a camada apelidada *Deep Web*, a qual é elaborada por redes de computadores que possuem como características principais o anonimato, a criptografia, a descentralização e a codificação aberta, fazendo com que os conteúdos então disponíveis sejam acessados por uma quantidade restrita de pessoas. Por fim, observa-se a *Dark Web*, uma subclassificação da *Deep Web*, que é marcada por um grau elevado de anonimato e pela manutenção da privacidade nas comunicações, sendo reconhecida pela sua alta taxa de práticas ilícitas e por sua carência de penalização.

Levando em consideração essa explicação concedida pelos autores do livro sobre as camadas da internet, verifica-se que ambientes como os da *Deep Web* são regularmente associados a atividades criminosas devido ao seu alto caráter de anonimato. Desse modo, é fundamental se atentar ao fato de que essa problemática não se instaura somente na teoria, em que é possível se trazer acontecimentos factuais desses vazamentos de dados na realidade. Isso

posto, observa-se através de uma notícia feita pela plataforma de cibersegurança, a "*Security Leaders*", em que especialistas da *Security Discovery* em conjunto com o portal *Cybernews* relataram o acontecimento no qual um agente desconhecido expôs na *Dark Web* um conjunto expressivo de 26 bilhões de dados sensíveis, retirando esses dados tanto de aplicativos quanto de organizações governamentais pelo mundo. Esse é um exemplo de como os usuários estão extremamente vulneráveis a despeito da existência de legislações que visam proteger esses dados. Com isso, evidencia-se que elas se configuram como ineficazes em acontecimentos com proporções desse porte, especialmente quando são efetuados em redes dificilmente fiscalizadas como a *Dark Web*.

Ademais, pode-se analisar o seguinte artigo da Lei Geral de Proteção de Dados:

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

I - a operação de tratamento seja realizada no território nacional.

À luz do artigo supracitado, identifica-se que a LGPD possui uma extraterritorialidade, isto é, ela abrange e manuseia dados pessoais de todos os indivíduos brasileiros, independente da origem e sede da empresa que comete o uso inadequado de dados dos usuários. Entretanto, levanta-se o seguinte questionamento: Se esse vazamento de dados foi efetuado por um indivíduo anônimo na *Deep Web*, como ele poderia ser penalizado, ainda que a vítima do vazamento seja brasileira? Tendo em vista esse questionamento, analisa-se que a sanção para a realização desse ato ilícito se encontra extremamente dificultada, especialmente partindo do pressuposto de que o espaço virtual não apresenta semelhanças ao espaço geográfico, mas sim devido ao fato de ser um espaço imaterial e consequentemente sem soberania (Marcondes Filho, 1996, p.100 *apud* Siqueira *et al.*, 2021). Assim, torna-se necessária a existência de uma cooperação internacional, algo que não é considerado uma alternativa para casos particulares, sendo que geralmente essa cooperação é ativada quando se apresenta um vazamento com uma proporção de dados elevada.

4. Considerações finais

Em suma, compreende-se que a Lei Geral de Proteção de Dados acaba não sendo eficaz para garantir a segurança de dados dos usuários em locais marcados pelo anonimato, como a *Deep Web*. Nesse contexto, infere-se que uma alternativa para amparar os indivíduos que tiveram suas informações expostas consiste na efetiva fiscalização da execução da LGPD pelas autoridades, com consequente responsabilização das empresas originalmente detentoras dessa exposição de dados, visando amenizar o dano causado às vítimas dessas exposições. Por fim, cabe mencionar que as conclusões desse estudo são preliminares e que a pesquisa se encontra em estágios iniciais de desenvolvimento mediante o referencial teórico e buscas na literatura.

Referências

BARRETO, A. G.; SANTOS, H. dos. **DEEP WEB: investigação no submundo da internet**. Rio de Janeiro: Brasport, 2019.

BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à Luz do Marco Civil da Internet**. Rio de Janeiro: Ed. Brasport, 2016. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=8k1PDQAAQBAJ&oi=fnd&pg=PA1&dq=Manual+de+Investiga%C3%A7%C3%A3o+Cibern%C3%A9tica+%C3%A0+Luz+do+Marco+Civil+da+Internet&ots=5tOrUaxdBb&sig=tuvVslMW_FdskNRY6cGC1c7pzhg#v=onepage&q=Manual%20de%20Investiga%C3%A7%C3%A3o%20Cibern%C3%A9tica%20%C3%A0%20Luz%20do%20Marco%20Civil%20da%20Internet&f=false. Acesso em: 14 maio. 2024.

CÉSAR, Daniel; JUNIOR, Irineu Francisco Barreto. **Marco civil da internet e neutralidade da rede: aspectos jurídicos e tecnológicos**. Revista Eletrônica do Curso de Direito da UFSM, v. 12, n. 1, p. 65-88, 2017. Disponível em: <https://periodicos.ufsm.br/revistadireito/article/view/23288/pdf>. Acesso em: 28 mar. 2024.

FERNANDES, Maria Luíza Batista *et al.* **Infiltração virtual de agentes policiais no combate aos crimes cibernéticos: ampliação na proteção da criança**. 2023. Disponível em: http://dspace.sti.ufcg.edu.br:8080/jspui/bitstream/riufcg/33137/1/MARIA%20LUIZA%20BATISTA%20FERNANDES%20-%20TCC%20%28Monografia%29%20Direito%20CCJS%202023_1_1%20%282%29.pdf. Acesso em: 28 mar. 2024.

KILIAN, Jean. **Crimes cibernéticos uma abordagem jurídica diante da eficácia na legislação brasileira**. 2020. Disponível em: <https://repositorio.unisc.br/jspui/bitstream/11624/2993/1/Jean%20Kilian.pdf>. Acesso em: 14 maio. 2024.

LIMA RAPÔSO, C. F.; MELO DE LIMA, H.; DE OLIVEIRA JUNIOR, W. F.; FERREIRA SILVA, P. A. .; ELAINE DE SOUZA BARROS, E. . **LGPD - Lei geral de proteção de dados pessoais em tecnologia da informação: Revisão sistemática**. RACE - Revista de Administração do Cesmac, [S. l.], v. 4, p. 58-67, 2019. DOI: 10.3131/race.v4i0.1035. Disponível em: <https://revistas.cesmac.edu.br/administracao/article/view/1035>. Acesso em: 14 maio. 2024.

MENDONÇA, Afonso Paulo Albuquerque de. **Novos instrumentos não eficazes de controle das tecnologias de comunicação e informação**. Revista Cidadania em Foco, v. 16, n. 1, 2022. Disponível em: <https://revista.tre-to.jus.br/tre-to/article/view/24/4>. Acesso em: 28 mar. 2024.

NEVES, Denise Lemes Fernandes *et al.* **A segurança da informação de encontro às conformidades da LGPD**. Revista Processando o Saber, v. 13, p. 186-198, 2021. Disponível em: <https://fatecpg.edu.br/revista/index.php/ps/article/view/171/146>. Acesso em: 28 mar. 2024.

SIQUEIRA, . N.; CONTIN, . C.; BARUFI, . B.; LEHFELD, . de S. **A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD**. REVISTA ELETRÔNICA PESQUISEDEUCA, [S. l.], v. 13, n. 29,

p. 236–255, 2021. DOI: 10.58422/repesq.2021.e1029. Disponível em:
<https://periodicos.unisantos.br/pesquiseduca/article/view/1029>. Acesso em: 14 maio. 2024.

SOARES DE SOUSA ARAÚJO, Y.; MARTINS CAVALCANTI, C.; DE LIMA MARQUES SANTIAGO SOUSA, V. **Comercialização Obscura na Era Digital: o tráfico internacional de crianças e adolescentes para fins de exploração sexual no Brasil à luz da Lei Geral de Proteção de Dados (LGPD)**. Cadernos Eletrônicos Direito Internacional sem Fronteiras, v. 5, n. 2, p. e20230206, 26 jul. 2023. Disponível em:
<https://www.cadernoseletronicosdisf.com.br/cedisf/article/view/161/132>. Acesso em: 14 maio. 2024.

SUCH, Gabriel Machtura et al. **Segurança e privacidade na internet**. Revista das Faculdades Santa Cruz, v. 11, n. 1, 2020. Disponível em: <https://periodicos.unisantacruz.edu.br/index.php/revusc/article/view/32/32>. Acesso em: 14 maio. 2024.