III CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL (III CIDIA)

RESPONSABILIDADE CIVIL E TECNOLOGIA

HELEN CRISTINA DE ALMEIDA SILVA

JOSÉ LUIZ DE MOURA FALEIROS JÚNIOR

LEDA LÚCIA SOARES

R434
Responsabilidade civil e tecnologia [Recurso eletrônico on-line] organização III Congresso Internacional de Direito e Inteligência Artificial (III CIDIA): Skema Business School – Belo Horizonte;

Coordenadores: José Luiz de Moura Faleiros Júnior, Leda Lúcia Soares e Helen Cristina de Almeida Silva – Belo Horizonte: Skema Business School, 2022.

Inclui bibliografia
ISBN: 978-65-5648-521-8
Modo de acesso: www.conpedi.org.br em publicações
Tema: A inteligência artificial e os desafios da inovação no poder judiciário.
1. Responsabilidade civil. 2. Inteligência artificial. 3. Tecnologia. I. III Congresso Internacional de Direito e Inteligência Artificial (1:2022 : Belo Horizonte, MG).

CDU: 34

III CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL (III CIDIA)

RESPONSABILIDADE CIVIL E TECNOLOGIA

Apresentação

O Congresso Internacional de Direito e Inteligência Artificial (CIDIA) da SKEMA Business School Brasil, que ocorreu em formato híbrido do dia 08 ao dia 10 de junho de 2022, atingiu a maturidade em sua terceira edição. Os dezesseis livros científicos que ora são apresentados à comunidade científica nacional e internacional, que contêm os 206 relatórios de pesquisa aprovados, são fruto das discussões realizadas nos Grupos de Trabalho do evento. São cerca de 1.200 páginas de produção científica relacionadas ao que há de mais novo e relevante em termos de discussão acadêmica sobre a relação da inteligência artificial e da tecnologia com os temas acesso à justiça, Direitos Humanos, proteção de dados, relações de trabalho, Administração Pública, meio ambiente, formas de solução de conflitos, Direito Penal e responsabilidade civil, dentre outros temas.

Neste ano, de maneira inédita, professores, grupos de pesquisa e instituições de nível superior puderam propor novos grupos de trabalho. Foram recebidas as excelentes propostas do Professor Doutor Marco Antônio Sousa Alves, da Universidade Federal de Minas Gerais (SIGA-UFMG – Algoritmos, vigilância e desinformação), dos Professores Doutores Bruno Feigelson e Fernanda Telha Ferreira Maymone, da Universidade do Estado do Rio de Janeiro (Metalaw – A Web 3.0 e a transformação do Direito), e do Professor Doutor Valmir Cézar Pozzetti, ligado à Universidade Federal do Amazonas e Universidade do Estado do Amazonas (Biodireito e tutela da vida digna frente às novas tecnologias).

O CIDIA da SKEMA Business School Brasil é, pelo terceiro ano consecutivo, o maior congresso científico de Direito e Tecnologia do Brasil, tendo recebido trabalhos do Amazonas, Bahia, Ceará, Distrito Federal, Espírito Santo, Goiás, Maranhão, Minas Gerais, Mato Grosso do Sul, Mato Grosso, Pará, Pernambuco, Piauí, Paraná, Rio de Janeiro, Rio Grande do Norte, Rio Grande do Sul, Santa Catarina, Sergipe e São Paulo. Tamanho sucesso não seria possível sem os apoiadores institucionais do evento: o CONPEDI – Conselho Nacional de Pesquisa e Pós-graduação em Direito, o Instituto Brasileiro de Estudos de Responsabilidade Civil – IBERC e o Programa RECAJ-UFMG - Ensino, Pesquisa e Extensão em Acesso à Justiça e Solução de Conflitos da Faculdade de Direito da Universidade Federal de Minas Gerais. Destaca-se, mais uma vez, a presença maciça de pesquisadores do Estado do Amazonas, especialmente os orientandos do Professor Doutor Valmir César Pozzetti.

Grandes nomes do Direito nacional e internacional estiveram presentes nos painéis temáticos do congresso. A abertura ficou a cargo do Prof. Dr. Felipe Calderón-Valencia (Univ. Medelín - Colômbia), com a palestra intitulada “Sistemas de Inteligência Artificial no Poder Judiciário - análise da experiência brasileira e colombiana”. Os Professores Valter Moura do Carmo e Rômulo Soares Valentini promoveram o debate. Um dos maiores civilistas do país, o Prof. Dr. Nelson Rosenvald, conduziu o segundo painel, sobre questões contemporâneas de Responsabilidade Civil e tecnologia. Tivemos as instigantes contribuições dos painelistas José Luiz de Moura Faleiros Júnior, Caitlin Mulholland e Manuel Ortiz Fernández (Espanha).

Momento marcante do congresso foi a participação do Ministro do Tribunal Superior do Trabalho – TST Maurício Godinho Delgado, escritor do mais prestigiado manual de Direito do Trabalho do país. Com a mediação da Profª. Drª. Adriana Goulart de Sena Orsini e participação do Prof. Dr. José Eduardo de Resende Chaves Júnior, parceiros habituais da SKEMA Brasil, foi debatido o tema “Desafios contemporâneos do gerenciamento algorítmico do trabalho”.

Encerrando a programação nacional dos painéis, o Prof. Dr. Caio Augusto Souza Lara, da SKEMA Brasil, dirigiu o de encerramento sobre inovação e Poder Judiciário. No primeiro momento, o juiz Rodrigo Martins Faria e a equipe da Unidade Avançada de Inovação do Tribunal de Justiça do Estado de Minas Gerais contaram sobre o processo de transformação em curso do Judiciário Estadual mineiro. Em seguida, o Prof. Dr. Fabrício Veiga Costa fez brilhante exposição sobre o projeto denominado “Processo Coletivo Eletrônico”, que teve a liderança do Desembargador Federal do Trabalho Vicente de Paula Maciel Júnior (TRT-3ª Região) e que foi o projeto vencedor do 18º Prêmio Innovare. O evento ainda teve um Grupo de Trabalho especial, o “Digital Sovereignty, how to depend less on Big tech?”, proposto pela Profª. Isabelle Bufflier (França) e o momento “Diálogo Brasil-França” com Prof. Frédéric Marty.

Os dezesseis Grupos de Trabalho contaram com a contribuição de 46 proeminentes professores ligados a renomadas instituições de ensino superior do país, os quais indicaram os caminhos para o aperfeiçoamento dos trabalhos dos autores. Cada livro desta coletânea foi organizado, preparado e assinado pelos professores que coordenaram cada grupo, os quais eram compostos por pesquisadores que submeteram os seus resumos expandidos pelo processo denominado double blind peer review (dupla avaliação cega por pares) dentro da plataforma PublicaDireito, que é mantida pelo CONPEDI.

Desta forma, a coletânea que ora torna-se pública é de inegável valor científico. Pretende-se, com ela, contribuir com a ciência jurídica e fomentar o aprofundamento da relação entre a graduação e a pós-graduação, seguindo as diretrizes oficiais da CAPES. Promoveu-se, ainda, a formação de novos pesquisadores na seara interdisciplinar entre o Direito e os vários campos da tecnologia, notadamente o da ciência da informação, haja vista o expressivo número de graduandos que participaram efetivamente, com o devido protagonismo, das atividades.

A SKEMA Business School é entidade francesa sem fins lucrativos, com estrutura multicampi em cinco países de continentes diferentes (França, EUA, China, Brasil e África do Sul) e com três importantes acreditações internacionais (AMBA, EQUIS e AACSB), que demonstram sua vocação para pesquisa de excelência no universo da economia do conhecimento. A SKEMA acredita, mais do que nunca, que um mundo digital necessita de uma abordagem transdisciplinar.

Agradecemos a participação de todos neste grandioso evento e convidamos a comunidade científica a conhecer nossos projetos no campo do Direito e da tecnologia. Foi lançada a nossa pós-graduação lato sensu em Direito e Tecnologia, com destacados professores e profissionais da área. No segundo semestre, teremos também o nosso primeiro processo seletivo para a graduação em Direito, que recebeu conceito 5 (nota máxima) na avaliação do Ministério da Educação - MEC. Nosso grupo de pesquisa, o Normative Experimentalism and Technology Law Lab – NEXT LAW LAB, também iniciará as suas atividades em breve.

Externamos os nossos agradecimentos a todas as pesquisadoras e a todos os pesquisadores pela inestimável contribuição e desejamos a todos uma ótima e proveitosa leitura!

Belo Horizonte-MG, 20 de junho de 2022.

Profª. Drª. Geneviève Daniele Lucienne Dutrait Poulingue

Reitora – SKEMA Business School - Campus Belo Horizonte

Prof. Dr. Edgar Gastón Jacobs Flores Filho

Coordenador dos Projetos de Direito da SKEMA Business School

OS IMPACTOS DOS VAZAMENTOS DE DADOS NA INTERNET A PARTIR DAS RELAÇÕES CONTRATUAIS

THE IMPACTS OF DATA LEAKS ON THE INTERNET FROM CONTRACTUAL RELATIONSHIPS

Lucas Oliveira Silva

Resumo

O artigo discutirá os vazamentos de dados pessoais na internet no âmbito das relações contratuais. Sabe-se que geralmente os contratos são feitos entre consumidores e grandes empresas, estando em clara desigualdade, gerando consequências para o contrato, o que será discutido no artigo. O assunto abordará a LGPD, além do Código Civil e o CDC, que regulam os contratos. A LGPD nos ajuda a visualizar os impactos que essa não proteção dos dados causam, de modo a gerar inúmeros danos aos titulares e às relações contratuais, alguns que violam a intimidade de modo drástico.

Palavras-chave: Lgpd, Vazamento de dados, Contratos na internet, Titular de dados

Abstract/Resumen/Résumé

The article will discuss the leaks of personal data on the internet in the context of contractual relationships. It is known that contracts are usually made between consumers and large companies, being in clear inequality, generating consequences for the contract, which will be discussed in the article. The subject will address the LGPD, in addition to the Civil Code and the CDC, which regulate contracts. The LGPD helps us to visualize the impacts that this non-protection of data causes, in order to generate numerous damages to the holders and to contractual relationships, some that violate privacy in a drastic way.

Keywords/Palabras-claves/Mots-clés: Lgpd, Data leakage, Contracts on the internet, Data holder

1. INTRODUÇÃO

A sociedade mundial vem presenciando, de modo cada vez mais rápido, transformações e evoluções tecnológicas em diversos campos, como das telecomunicações, das missões espaciais e dos equipamentos de uso pessoal. O Brasil também se atualizou em relação ao movimentado mundo tecnológico não só com desenvolvimento de tecnologia, mas também ao promulgar uma Lei sobre proteção e privacidade de dados pessoais (Lei nº 13.709/18). Esta Lei, porém, foi publicada com anos de atraso, se considerarmos legislações sobre o tema promulgadas anos atrás, como o europeu "convenio 108", datado de 28 de janeiro de 1981, que anos mais tarde daria luz ao Regulamento Geral sobre a Proteção de Dados.

Essa evolução do acesso à tecnologia no Brasil hoje está alcançando níveis nunca visto, considerando o crescimento do acesso cada vez mais facilitado aos computadores, ao ensino tecnológico e às redes de informação. Sabe-se, porém, que a internet pode trazer inúmeros riscos à segurança dos usuários, considerando que informações são trocadas e inseridas ao se realizar transações bancárias, fazer compras ou navegar na rede por mero entretenimento.

Com a Lei 13.709/18, ora citada, conhecida como LGPD (Lei Geral de Proteção de Dados Pessoais), deseja-se que esses acessos à rede mundial de computadores sejam realizados com a maior segurança possível, assegurando os direitos dos usuários. Ela, portanto, é um marco para o Brasil, pois modernizou o país na proteção dos dados pessoais. Além disso, a Emenda Constitucional nº 115, de 2022, inseriu a proteção desses dados no rol de direitos fundamentais do art. 5º (inciso LXXIX) da Constituição Federal. Esta conquista mostra a importância que o Estado Brasileiro dá no tocante à proteção dos dados adquiridos no Brasil. Além disso, quando se refere a navegar na rede mundial de computadores, fala-se também de negócios que são feitos e contratos celebrados.

Portanto, há um perigo nisso tudo quando falamos em dados trocados na internet, pois quando esses dados são utilizados para outras finalidades diferentes das acordadas, temos uma violação do direito à privacidade de dados pessoais. Tal violação gera prejuízos ao titular que podem assumir grandes proporções. Esses efeitos alcançam também os contratos, pois tais violações terão consequências diversas no âmbito deste instrumento, sendo tratada mais a fundo durante o desenvolvimento do artigo.

2. OBJETIVOS

O objetivo macro do artigo é entender os impactos dos vazamentos de dados na internet a partir das relações contratuais, de modo que se saiba como lidar com essas consequências. Para alcançar esse objetivo, deve-se entender em que medida se aplica sanções para os vazamentos de dados pessoais, previstas na LGPD, entender as questões que envolvem os contratos, como extinção, resolução e formação dos contratos, além de enxergar o assunto proposto à luz das duas perspectivas.

3. METODOLOGIAS

O método aplicado, considerando que o objetivo é entender como que o direito contratual se comporta diante da LGPD e do vazamento de dados pessoais, é o de pesquisa exploratória. Há a necessidade, para um correto entendimento do tema, de pesquisar e explicar os fenômenos que surgem das relações contratuais no âmbito da LGPD. Desse modo, levantar-se-á material bibliográfico e análise de *cases* ocorridos não só no Brasil como ao redor do mundo, caso tenha pertinência com o tema.

4. DESENVOLVIMENTO DA PESQUISA

4.1. RELAÇÕES CONTRATUAIS NA INTERNET E APLICAÇÃO DA LGPD

Os contratos são necessários para que se exerçam negócios jurídicos entre duas ou mais pessoas, sejam físicas ou jurídicas. É por meio dele que as partes expressam as suas vontades e interesses em torno de um objeto. Por meio desse instrumento, criam-se obrigações entre os contratantes, tornando-se válidas perante a ordem jurídica. O professor Paulo Nader (2018, p. 2) disciplina sobre a definição de Contrato:

> Contrato é modalidade de fato jurídico, mais especificamente, de negócio jurídico bilateral ou plurilateral, pelo qual duas ou mais vontades se harmonizam a fim de produzirem resultados jurídicos obrigacionais, de acordo com o permissivo e limites da lei.

Sabe-se que o Código Civil possui uma gama de normas que regulam os contratos, sendo os mais notáveis os princípios norteadores que são a Probidade e Boa Fé (art. 422, CC), a Autonomia da Vontade (art. 421, CC), a Supremacia da Ordem Pública e da Revisão dos Contratos (art. 478, 479 e 480 CC), por exemplo.

Há diversas espécies dentro dessas relações contratuais, que inclusive estão dispostas no Código Civil (art. 481 a 853). Dentre os que são mais comuns, destaca-se o Contrato de Adesão, que

normalmente é feito em diversas relações na rede mundial de computadores, principalmente nos nas relações de consumo, e consiste em, segundo Orlando Gomes (1998, p. 109), aceitar, “em bloco, as cláusulas estabelecidas pela outra, aderindo uma situação contratual que encontra definida em todos os seus termos”.

Relacionando isso à LGPD, sabe-se que há dados compartilhados entre as partes contratantes a fim de efetivar o contrato e permitir que serviços sejam prestados e compras sejam feitas. No entanto, esse compartilhamento de dados pessoais é feito de modo que atendam aos princípios da LGPD, como o que está exposto no art. 6º: Finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

Quando se houver uma inadequação em relação à LGPD relacionado a esse contrato firmado, haverá consequências negativas ao contrato, a ser avaliada na medida dos prejuízos causados.

4.2. DANOS GERADOS AO TITULAR DOS DADOS: AS SANÇÕES SÃO ADEQUADAS AOS PREJUÍZOS CAUSADOS?

Antes de falar sobre os problemas advindos, é necessário discorrer sobre a falta se segurança nesses ambientes, que é a responsável pelo problema. Sabe-se que a segurança no ambiente cibernético é de suma importância, considerando as peculiaridades da internet, onde tudo é conectado. O art. 6º da LGPD, inclusive, estabelece como princípio a segurança nos ambientes de tratamento de dados, tamanha a importância do tema:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> (...)
>
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

Em uma pesquisa realizada em 2022, pela BugHunt (2021, p. 9), com 130 empresas de todos os continentes, constatou-se que 45% das empresas já haviam sofrido ataques cibernéticos, sendo estes por Vírus (24%), *Ramsonware* (21%), *Vishing* (10%) e *Phishing* (28%). Destaca-se, entre os tipos de ataques citados na pesquisa, o *Phishing*, pois possui a maior porcentagem de ocorrência e consiste em “pescar” o seu destinatário por meio de links, a fim de roubar dados pessoais, como nome, CPF e dados de cartão de crédito.

Os atacantes, no entanto, nem sempre querem dados pessoais, pois podem roubar dados comerciais e causar danos descomunal à uma determinada sociedade empresária. Pesquisas demonstram que esse tipo de ataque é cada vez mais buscado, pois, apesar de não causar violações de direitos sobre dados pessoais, causa danos à imagem das empresas, além da perda de oportunidades de negócios e aumento do custo com segurança da informação. Segue trecho da pesquisa do NIC.BR (Núcleo de Informação e Coordenação do Ponto BR) (2020, p. 25) sobre o prejuízo das empresas:

> De acordo com o relatório de 2019 da empresa de consultoria PwC para a Comissão Europeia, o roubo digital relativo à segurança de segredos comerciais na Europa, em 2018, resultou em perdas de 60 bilhões de euros para o crescimento econômico e quase 289 mil empregos perdidos; além disso, projeções para 2025 ascendem a um milhão de perdas de empregos14. O roubo de segredos comerciais pode levar a custos significativos de oportunidade, impactos negativos na inovação, aumento de gastos em segurança e danos à reputação

Ademais, segundo pesquisas feitas pelo Grupo MZ (2021, p. 5), empresa especializada em relações com investidores, entre janeiro de 2020 e fevereiro de 2021, por conta do aumento exponencial do Home Office ocasionado pela pandemia de Covid-19, o número de ataques cibernéticos a empresas brasileiras cresceu 220.

Desse modo, extrai-se que as empresas não estavam preparadas para implementar o trabalho remoto com segurança, abrindo, assim, brechas para que os atacantes roubem dados e informações dos usuários.

Essas ações dos criminosos não geram somente perdas de dados pessoais, mas, caso a empresa tenha culpa na exposição desses dados ou na falta de segurança implementada, ela também responde judicialmente, nos termos do art. 52 da LGPD.

As relações contratuais geram direitos e deveres para as partes contratantes, assim diz o famoso brocardo em latim "*Pacta Sunt Servanda*", que pode ser reproduzido por "o contrato faz lei entre as partes". Desse modo, deve-se respeitar os contratos e cumprir as cláusulas contidas neles. Considerando o vazamento de dados, há sanções não só para quando não se respeitam os contratos em sentido estrito, como também os direitos e garantias respaldados, principalmente, na Constituição Federal. A LGPD estipula, na seção II, as Sanções Administrativas atreladas ao cometimento de infrações contra os titulares de dados. Essas multas pecuniárias são consideráveis, pois podem chegar a cifras milionárias, como o inciso II do art. 52 dispõe:

> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos

> os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

Além da multa do inciso II, o artigo 52 estipula outras sanções como advertência, a multa diária, eliminação dos dados pessoais a que se refere a infração e proibição de se utilizar os dados por 06 meses, por exemplo.

5. CONCLUSÕES

Há inúmeros impactos nos contratos decorrentes de vazamento de dados, sendo, em último caso, passível de resolução, nos termos do Código Civil. O que deve ser levado em conta, no entanto, são os impactos que esse incidente causou às partes envolvidas. Sabe-se que nas relações contratuais os dados podem ser tratados, quando estes são necessários, sendo comum que esses dados, a partir do momento que são compartilhados, estão passíveis de serem vazados, pois não há que se falar em segurança ideal em segurança da informação. Desse modo, conclui-se que os vazamentos, nos contratos, podem ser inúmeros, como a resolução do contrato entre as partes, considerando um efeito interno, o uso desses dados por agentes mal-intencionados, venda desses dados, exposição das partes com dados pessoais comuns e sensíveis, considerando os impactos externos ao contrato. Além disso, há impacto também para os que incorrem em culpa na violação desses dados pessoais, como a incumbência de arcar com custos da resolução dos contratos, indenizar as vítimas, arcar com os custos de reparação dos prejuízos e arcar com as sanções previstas no art. 52 da LGPD, que inclui advertência, multa de até R$50.000.000,00 (cinquenta milhões de reais) por infração, multa diária e publicização. Todos esses impactos são adequados e devem ser utilizados como parâmetros em contratos celebrados na rede mundial de computador, considerando a disponibilidade e aplicabilidade de uma Lei Geral de Proteção de Dados Pessoais.

6. REFERENCIAIS

LÔBO, Paulo Luiz N. **Direito Civil Volume 3 - Contratos**. São Paulo: Editora Saraiva, 2022. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555596793/. Acesso em: 05 mai. 2022.

NADER, Paulo. **Curso de Direito Civil - Vol. 3 - Contratos, 9ª edição**. Rio de Janeiro: Grupo GEN, 2018. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530979621/. Acesso em: 05 mai. 2022.

GOMES, Orlando. **Contratos**, 18ª edição. Rio de Janeiro: Forense, 1998.

BUGHUNT (comp.). **Segurança da Informação no Brasil**: 1ª pesquisa nacional bughunt de segurança da informação. São Paulo, 2020. 17 p. Disponível em: <https://drive.google.com/file/d/17tCFv70fFsss7R8v7FcXq04mJp1YbyEd/view>. Acesso em: 19 mar. 2022.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (org.). **Segurança digital:** uma análise da gestão de riscos em empresas brasileiras. São Paulo: Comitê Gestor da Internet no Brasil, 2020. Disponível em: <https://cetic.br/media/docs/publicacoes/7/20210514123130/estudos-setoriais-seguranca-digital.pdf>. Acesso em: 29 mar. 2022.

MZ GROUP. **Monitoramento de Mercado:** ataques cibernéticos: janeiro de 2020 a fevereiro de 2021. São Paulo: Mz Consult, 2021. Disponível em: <https://api.mziq.com/mzfilemanager/v2/d/8136baea-90cc-46fc-9bc0-4a1f25f52a53/f7acc4b2-5ea0-cdc7-92f7-34c027c57808?origin=1>. Acesso em: 02 abr. 2022.