II CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL

TECNOLOGIAS DISRUPTIVAS, DIREITO E PROTEÇÃO DE DADOS II

T255
Tecnologias Disruptivas, Direito e Proteção de Dados - II [Recurso eletrônico on-line] organização Congresso Internacional de Direito e Inteligência Artificial: Skema Business School – Belo Horizonte;

Coordenadores: Caio Augusto Souza Lara; Wilson de Freitas Monteiro; José Luiz de Moura Faleiros Júnior. – Belo Horizonte:Skema Business School, 2021.

Inclui bibliografia
ISBN: 978-65-5648-269-9
Modo de acesso: www.conpedi.org.br
Tema: Um olhar do Direito sobre a Tecnologia

1. Direito. 2. Inteligência Artificial. 3. Tecnologia. II. Congresso Internacional de Direito e Inteligência Artificial (1:2021 : Belo Horizonte, MG).

CDU: 34

II CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL

TECNOLOGIAS DISRUPTIVAS, DIREITO E PROTEÇÃO DE DADOS II

Apresentação

Renovando o compromisso assumido com os pesquisadores de Direito e tecnologia do Brasil, é com grande satisfação que a SKEMA Business School e o CONPEDI – Conselho Nacional de Pesquisa e Pós-graduação em Direito apresentam à comunidade científica os 12 livros produzidos a partir dos Grupos de Trabalho do II Congresso Internacional de Direito e Inteligência Artificial (II CIDIA). As discussões ocorreram em ambiente virtual ao longo dos dias 27 e 28 de maio de 2021, dentro da programação que contou com grandes nomes nacionais e internacionais da área em cinco painéis temáticos e o SKEMA Dialogue, além de 354 inscritos no total. Continuamos a promover aquele que é, pelo segundo ano, o maior evento científico de Direito e Tecnologia do Brasil.

Trata-se de coletânea composta pelos 255 trabalhos aprovados e que atingiram nota mínima de aprovação, sendo que também foram submetidos ao processo denominado double blind peer review (dupla avaliação cega por pares) dentro da plataforma PublicaDireito, que é mantida pelo CONPEDI. Os oito Grupos de Trabalho originais, diante da grande demanda, se transformaram em doze e contaram com a participação de pesquisadores de vinte e um Estados da federação brasileira e do Distrito Federal. São cerca de 1.700 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.

Os referidos Grupos de Trabalho contaram, ainda, com a contribuição de 36 proeminentes professoras e 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. Sem dúvida, houve uma troca intensa de saberes e a produção de conhecimento de alto nível foi, mais uma vez, o grande legado do evento.

Neste norte, a coletânea que ora torna-se pública é de inegável valor científico. Pretende-se, com esta publicação, contribuir com a ciência jurídica e fomentar o aprofundamento da relação entre a graduação e a pós-graduação, seguindo as diretrizes oficiais. Fomentou-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. Já está em funcionamento o projeto Nanodegrees, um conjunto de cursos práticos e avançados, de curta duração, acessíveis aos estudantes tanto de graduação, quanto de pós-graduação. Em breve, será lançada a pioneira pós-graduação lato sensu de Direito e Inteligência Artificial, com destacados professores da área. A SKEMA estrutura, ainda, um grupo de pesquisa em Direito e Inteligência Artificial e planeja o lançamento de um periódico científico sobre o tema.

Agradecemos ainda a todas as pesquisadoras e pesquisadores pela inestimável contribuição e desejamos a todos uma ótima e proveitosa leitura!

Belo Horizonte-MG, 09 de junho de 2021.

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

SEGURANÇA DIGITAL JURÍDICA: QUEM ESTÁ NO CONTROLE?

LEGAL DIGITAL SECURITY: WHO IS IN CONTROL?

João Paulo Silva Costa [1]

Resumo

Esta pesquisa abordará a segurança digital do sistema judiciário brasileiro, no âmbito do Direito Digital, sob a luz do recente sequestro de dados do STJ. A partir disso, é possível concluir como o cenário brasileiro possui um despreparo grave em relação ao cenário internacional de proteção de conteúdo digital, o que poderia atrasar consideravelmente processos importantes, bem como dar margem para alterações nos documentos processuais. Para tanto, a vertente metodológica de pesquisa utilizada é a jurídico-social, sendo o tipo jurídico-projetivo utilizado no tocante ao tipo de investigação, tendo o raciocínio dialético predominante na pesquisa.

Palavras-chave: Segurança digital, Direito digital, Stj, Defasagem

Abstract/Resumen/Résumé

This research will adress the digital security of the brazilian judicial system, within the scope of Digital Law, under the light of the recent data kidnap from the STJ. From that, it is possible to conclude how the brazilian scenery of digital content protection has a serious unpreparedness comparing to the international's one, what could delay important law suits, as well as giving an opening to alterations in it's documents. Therefore, the research methodological approach used is the juridical-sociological, being the legal-projective type the one used on the investigation type, having the dialectical reasoning as the predominant in this research.

Keywords/Palabras-claves/Mots-clés: Digital security, Stj, Unpreparedness, Digital law

[1] Graduando em Direito - modalidade Integral - pela Escola Superior Dom Helder Câmara.

1. CONSIDERAÇÕES INICIAIS

A presente pesquisa tem como objetivo demonstrar as consequências da defasagem do sistema virtual de segurança do judiciário brasileiro, estabelecendo uma ponte com o processo de digitalização do Direito e com um enfoque principal no caso de ataque *ransomware* ao Supremo Tribunal de Justiça (STJ).

Devido ao intenso avanço da tecnologia, a área jurídica não poderia deixar de ser afetada, uma vez que, com o crescente uso de novas ferramentas digitais em diversos setores e com a crise ocasionada pela pandemia do Covid-19, era inevitável a digitalização do Direito e de seus conteúdos processuais, estabelecendo novas vertentes judiciais e refutando os ideais contrários ao estabelecimento de uma conexão entre tecnologia e Direito. (COELHO, 2020)

Convém ressaltar, dessa forma, que as consequências dessas transformações não serão necessariamente positivas, já que o meio virtual jurídico abre um novo caminho para a prática de crimes cibernéticos, os quais podem afetar a sociedade como um todo, não somente o ramo do Direito.

Em suma, essa pesquisa pretende estabelecer um novo olhar sobre a gravidade dos problemas ocasionados pelas práticas de sequestro de dados e outros crimes virtuais que podem afetar os processos no país, demonstrando como estas ilegalidades podem fragilizar o sistema, além de passar o controle da justiça para as mãos daqueles que dominam mais a área digital.

A pesquisa que se propõe, na classificação de Gustin, Dias e Nicácio (2020), pertence à vertente metodológica jurídico-social. No tocante ao tipo genérico de pesquisa, foi escolhido o tipo jurídico-projetivo. O raciocínio desenvolvido na pesquisa é predominantemente dialético e quanto ao gênero de pesquisa, foi adotada a pesquisa teórica.

2. DIGITALIZAÇÃO DO DIREITO

Inicialmente, é necessário compreender as mudanças que atingem o mundo da informática, sendo a humanidade hoje uma testemunha do que a globalização é capaz de desenvolver. Com efeito, isso pode ser percebido desde o desenvolvimento das primeiras formas de comunicação à distância até o advento da Internet, sendo esta uma rede capaz de conectar diferentes locais em uma única rede global (GOUVÊA, 1997).

Nesse sentido, é oportuno salientar como a digitalização das atividades no contexto social vem sendo aplicada por meio de mudanças e exigências de diferentes setores, com o objetivo principal de melhorar a produtividade, tornando tais atividades mais práticas e eficientes (PINHEIRO, 2021).

Dessa forma, novas exigências são formadas na área jurídica, como foi descrito pela especialista em Direito Digital, doutorada pela Universidade de São Paulo, Patrícia Peck Pinheiro:

> Assim, começam a surgir propostas de regulamentação em todo o mundo para que se crie um quadro jurídico mais robusto (framework legal), visto que já convivemos com muitos robôs de assistência médica e de sistemas de vigilância. Surge da necessidade de se estabelecer regras que considerem o impacto ético e social dessas novas tecnologias, afinal, a próxima geração de robôs é muito mais autônoma e tem a capacidade de aprendizagem com coleta de dados. (PINHEIRO, 2021, n.p)

Depreende-se, portanto, como a atuação judiciária moderna é desenvolvida para acompanhar as mudanças digitais, que começaram a surgir desde o desenvolvimento da internet e dos primórdios da computação. Segundo dados do Conselho Nacional de Justiça (CNJ), 108 milhões de causas tiveram início em versão digital de 2008 para 2018, além de que 100% dos processos na Justiça do Trabalho já são eletrônicos (VASCONCELOS, 2020).

A partir destas transformações é inegável a confirmação de uma forma de trabalho mais prática, possibilitando uma maior agilidade no desenvolvimento de processos e até mesmo o desenvolver de audiências virtuais. No entanto, novas práticas criminosas também se desencadearam durante esse fenômeno, o que pode ser claramente exemplificado com o sequestro de dados ao Superior Tribunal de Justiça (STJ).

Em suma, o processo da digitalização do Direito se tornou mais do que essencial para o mundo contemporâneo, possibilitando uma celeridade essencial ao Poder Judiciário, além de trazer novas exigências ao Estado, uma vez que este torna-se responsável por regular as novas transformações oriundas da revolução tecnológica. É imprescindível uma visão da informação e dos dados como bens jurídicos, independentemente do conteúdo trazido por estes (GOUVÊA, 1997).

2. INTELIGÊNCIA ARTIFICIAL E CRIMES VIRTUAIS NO DIREITO

Ao estabelecer uma ligação sólida entre a revolução digital e o mundo jurídico atual, diversas são as transformações e consequências geradas. Com efeito, a aplicação da inteligência artificial (IA) e a utilização do *machine learning* estão se tornando cada vez

mais frequentes, sendo estas medidas práticas que visam agilizar o processo judicial e satisfazer as exigências recorrentes do "mundo líquido" [1].

No âmbito da advocacia, um exemplo relevante é a inteligência artificial ROSS, um robô advogado. Este consiste em uma fonte para consultas jurídicas em jurisprudências e legislações, que utiliza métodos de aprendizagem baseados em *machine learning.* Tratando-se de resultados, escritórios que aplicaram esta IA afirmaram uma redução de 30% no tempo de pesquisa, encontrando resultados 40% mais relevantes. É imprescindível, pois, a utilização de artifícios como este nos maiores centros de aplicação jurídica, como nos tribunais de justiça estaduais e até mesmo o próprio Supremo Tribunal Federal (STF) (HOFFMAN, 2018, p. 43).

É importante considerar, ainda, como a utilização de juízes artificias pode desempenhar mudanças significativas no âmbito jurídico. Para tanto, uma melhor compreensão do papel desempenhado por estes torna-se necessária. Segundo Hoffman:

> Assim, considerando que os juízes, ao analisar determinadas matérias – várias presentes naquelas objeto das Ações de Massa – exercem uma espécie de inteligência artificial, atuando como máquinas, embora sem a velocidade e eficiência das plataformas de sistemas inteligentes, parece inexistir óbice à aplicação de Inteligências Artificiais para análise, processamento e apoio à decisão, ao menos no âmbito das lides de baixa complexidade (HOFFMAN, 2018, p. 54, 55).

A partir disto, a preocupação com crimes cibernéticos tende a se tornar cada vez mais relevante, uma vez que na nova era digital estes são capazes de controlar os rumos da justiça se aplicados da maneira correta. Os resultados de tais delitos podem ser gravíssimos, como pode ser exemplificado pela quebra do Banco Nacional, a qual ocorreu como consequência de uma fraude que perdurou por anos, em que os funcionários do alto escalão mantiveram contas fictícias através de um microcomputador não conectado ao sistema central, o que ocultava os balanços do banco e apresentava lucros fictícios (GOUVÊA, 1997, p. 26).

Tendo em vista tais fatos, a prática de artifícios maliciosos no meio digital deixa de ser uma preocupação apenas com a segurança de organizações estaduais e grandes empresas privadas, as quais visam proteger seus dados, e passa a se tornar uma preocupante inimiga do próprio Direito, tendo em vista que no cenário da digitalização do sistema judiciário em diferentes âmbitos, quem possui o maior conhecimento tecnológico é capaz de tomar o controle, seja por meio de invasões que roubem dados importantes para a conclusão de processos ou com

[1] BAUMAN, Zigmund. **Modernidade Líquida. 1.** Ed. Rio de Janeiro: Zahar, 2001.

a utilização de programas capazes de controlar a decisão de juízes artificiais, o que desconfigura a prática democrática do sistema judiciário.

Nesse sentido, é importante considerar como a investigação criminal de ataques como estes é cada vez mais dificultada, em face ao fortalecimento da proteção da confidencialidade, por meio de diferentes técnicas de criptografia, que se fazem presentes em diversos programa e produtos. Tal fator provoca a utilização de artefatos como o *malware,* um programa informático controverso capaz de ser instalado de maneira oculta em seu alvo e recolher dados armazenados. Entretanto, como este representa um método encoberto, a sua aplicação é capaz de gerar uma controvérsia, uma vez que tal artifício não é capaz de proteger, necessariamente, os direitos fundamentais das pessoas perante o Estado (CAMPOS, 2021, p. 13,14).

Uma vez que os métodos para proteção de ataques ao sistema judiciário não são capazes de se estabelecer de uma maneira concreta e completamente dentro da legalidade, no contexto da utilização do *malware,* este mesmo artifício é capaz de ser utilizado para a prática de crimes contra o próprio sistema judiciário, como foi o caso do ataque ao STJ, executado por meio de um *ransomware*, o que paralisou o tribunal por cerca de 6 dias, existindo, ainda, a possibilidade de vazamentos de dados, o que poderia prejudicar não somente o cenário nacional, como colocar em risco a privacidade internacional do Brasil.

Sendo assim, pode ser depreendido como o cenário brasileiro atual ainda se encontra em um estado de defasagem no tocante a segurança digital jurídica, sendo incapaz de se proteger de maneira efetiva e possibilitando um estado crítico de incapacitação e insegurança ao próprio Direito brasileiro. O problema consiste em uma negligência de estratégias de prevenção, o que já pode se fazer claro durante o seminário “Meet the Enemy”, do *Computer Security Institute* em Chicago, em que diversos hackers afirmaram que é fácil invadir os computadores no Brasil, uma vez que aqui não existe uma preocupação séria com a segurança da informação (NERY, 1997, p. 22).

3. O CASO STJ E SUAS IMPLICAÇÕES NO CENÁRIO DO DIREITO

A invasão ao Supremo Tribunal de Justiça, no dia 3 de novembro de 2020, que utilizou um *ransomware* para sequestrar e criptografar arquivos importantes do sistema, além de atingir diretamente os e-mails do STJ, foi capaz de impossibilitar um dos maiores tribunais do país de exercer sua função básica: julgar processos. Com efeito, tal ciberataque ainda foi acompanhado

de um arquivo de texto dando instruções para a recuperação dos arquivos por meio de pagamentos, correspondendo ao ideal da baixa segurança digital dos órgãos brasileiros.

O processo da digitalização no STJ foi líder no judiciário, por meio do programa "STJ na Era Virtual", desenvolvido em 2009. Como efeito disso, o "e-STJ", foi capaz de reduzir custos de transporte, impressão e armazenamento de papel, tendo como consequência principal, 10 anos depois, o estabelecimento do processo eletrônico e uma tramitação digital como regra em todo o sistema judiciário. Ainda que tal fato seja capaz de representar um grande avanço para o Direito brasileiro, o país não deixa de estar atrasado na era da digitalização, o que pode ser corroborado com o próprio ataque *ransomware* (SALVADOR; GUIMARÃES, 2020)

O sequestro de dados, em conjunto com suas diversas implicações negativas, foi capaz de apontar uma grave falha em todo o sistema judiciário brasileiro: Uma negligência gravíssima com a segurança digital. Segundo o que foi descrito por Salvador e por Guimarães:

> O que mais impressiona no ataque ao STJ é que justamente uma das instituições mais importantes para o funcionamento do Judiciário brasileiro e mais experientes no campo da digitalização se revelou despreparada para lidar com um problema que já tem vários anos de vida. Já em 2017, quando o *ransomware* WannaCry causou danos milionários em todo o globo, tribunais brasileiros e outros órgãos atingidos, ainda que em menor escala. Hoje, o Brasil é líder global em número de empresas atacadas por *ransomware* durante a pandemia. Ciberataques desse tipo não são novos no país e as estratégias de prevenção já deveriam estar difundidas.

Mesmo que o caso STJ não tenha implicado em consequências extremante prejudiciais à população brasileira, nem todos os ataques cibernéticos são 'inofensivos", uma vez que para o lado das vítimas desses ataques com o uso de *malwares* os custos podem ser imensuráveis, podendo significar o fim de uma empresa de pequeno porte ou, no caso de instituições estaduais, a impossibilidade de o Estado exercer seu papel de garantia aos direitos fundamentais, no caso referido, o direito à justiça. Em casos mais extremos, até a morte pode ser uma implicação, como o que ocorreu com uma pessoa na Alemanha por não poder ser atendida devido a complicações originada de um ataque cibernético (SALVADOR; GUIMARÃES, 2020).

Conclui-se, portanto, que o Brasil não está completamente preparado para se defender de ataques cibernéticos, o que pode gerar sérias consequências negativas ao próprio Direito, uma vez que, no contexto de um sistema judiciário indefeso, o próprio conceito da aplicação efetiva de procedimentos jurídicos perde completamente sua credibilidade, além do risco de espionagem internacional por meio do roubo de dados, colocando o país em uma preocupante posição de desvantagem.

4. CONSIDERAÇÕES FINAIS

Tendo em vista o que foi exposto, é possível perceber que com o processo de digitalização do Direito, muitos avanços foram estabelecidos no sistema judiciário brasileiro, tornando mais prática e efetiva a vida dos juristas. Ainda assim, tal fenômeno cresceu de maneira paralela ao desenvolvimento de diferentes artifícios para a realização de crimes virtuais, como o próprio *malware*. Nesse sentido, no contexto da utilização de inteligências artificiais e outros meios virtuais da aplicação jurídica, o cenário do país se encontra em grande risco, devido a perpetuação de sua defasagem de segurança digital.

Além disso, é de extrema importância analisar como o investimento para a proteção de dados é extremamente necessário, como medida preventiva a ataques como o praticado contra o STJ ou até mesmo contra o Tribunal de Justiça do Rio Grande do Sul, os dois realizados de maneiras análogas, com o uso de *ransomwares*, trazendo consequências, também, semelhantes, com o atraso de processos e inutilização do tribunal durante um período de tempo.

É necessário considerar, dessa forma, as medidas tomadas pelo país para conter a prática de tais delitos e proteger tanto a Segurança Nacional quanto os direitos fundamentais da população. Com efeito, isso pode ser corroborado com a promulgação da Estratégia Nacional de Segurança Cibernética, em 2020, propondo a criação de um sistema que efetive a segurança cibernética e cobre do Estado atitudes estratégicas como o incentivo a soluções inovadoras. A própria LGPD (Lei Geral de Proteção de Dados) é capaz de entrar neste contexto, como uma forma de garantia de padrões mínimos de proteção (SALVADOR; GUIMARÃES, 2020).

Por fim, é possível extrair que não se deve mais adiar e negligenciar as estratégias de prevenção e proteção a segurança digital jurídica no Brasil. As consequências ocasionadas por crimes cibernéticos já se mostraram extremamente graves, atingindo indiretamente toda a população e colocando o país em situação de risco no âmbito de proteção de dados e segurança nacional. O Estado no mundo digitalizado deve se precaver cada vez mais para continuar garantindo o monopólio do uso do Direito, impossibilitando que aqueles que possuam um maior arsenal cibernético sejam os verdadeiros controladores da justiça no país.

5. REFERÊNCIAS

CAMPOS, Juliana Filipa Sousa. ***O Malware como Meio de Obtenção da Prova em Processo Penal***. 1ª. ed. Coimbra: ALMEDINA, 2021.

COELHO, Alexandre Zavaglia. A transformação digital na área do Direito. ***Consultor Jurídico***, São Paulo 12 de maio 2020. Disponível em: https://www.conjur.com.br/2020-mai-12/alexandre-coelho-transformacao-digital-direito. Acesso em 03 de maio de 2021.

GOUVÊA, Sandra. ***O Direito na Era Digital: Crimes Praticados por meio da Informática***. 1ª. ed. Rio de Janeiro: Mauad, 1997.

GUSTIN, Miracy Barbosa de Sousa; DIAS, Maria Tereza Fonseca; NICÁCIO, Camila Silva. ***(Re)pensando a pesquisa jurídica: teoria e prática***. 5ª. ed. São Paulo: Almedina, 2020.

HOFFMAN, Alexandra Felipe. ***DIREITO E TECNOLOGIA: A UTILIZAÇÃO DE INTELIGÊNCIAS ARTIFICIAIS NO PROCESSO DECISÓRIO.*** 2018. 62. Trabalho de Conclusão de Curso (Graduação em Direito) – Curso de Direito -Universidade Federal de Santa Catarina, Santa Catarina, 2018.

PINHEIRO, Patrícia Peck. et al. ***Segurança Digital: Proteção de Dados nas Empresas***. 1ª. ed. Belo Horizonte: Atlas, 2020

SALVADOR, João Pedro Favaretto; GUIMARÃES, Tatiane. O ataque ao STJ é mais um grito de socorro da segurança cibernética no Brasil. ***Portal FGV,*** São Paulo 9 novembro 2020. Disponível em: https://portal.fgv.br/artigos/ataque-ao-stj-e-mais-grito-socorro-seguranca-cibernetica-brasil. Acesso em 2 maio de 2021.

VASCONCELOS, Esther. Transformação Digital: Houve grande avanço na digitalização de processos no judiciário. ***Rede Jornal Contábil,*** São Paulo, 10 de agosto de 2020. Disponível em: https://www.jornalcontabil.com.br/transformacao-digital-digitalizacao-de-processos-no-judiciario/. Acesso em 4 de maio de 2021.