VI ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

DANIELLE JACON AYRES PINTO

EDSON RICARDO SALEME

FERNANDO GALINDO AYUDA

D597

Direito, governança e novas tecnologias II [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Danielle Jacon Ayres Pinto; Edson Ricardo Saleme; Fernando Galindo Ayuda – Florianópolis; CONPEDI, 2023.

Inclui bibliografia
ISBN: 78-65-5648-746-5
Modo de acesso: www.conpedi.org.br em publicações
Tema: Direito e Políticas Públicas na era digital

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. VI Encontro Virtual do CONPEDI (1; 2023; Florianópolis, Brasil).

CDU: 34

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

VI ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

Apresentação

Apresentação do CONPEDI – novas tecnologias.

O grupo constituído por DANIELLE JACON AYRES PINTO, FERNANDO GALINDO e EDSON R. SALEME presidiram o GT Direito, Governança e novas tecnologias II, que tiveram o privilégio de conduzir excelentes trabalhos apresentados, que apontaram as necessidades brasileiras mais prementes, em termos normativos, na era digital. Os trabalhos abordaram as características mais marcantes que estão sujeitos os dados, sobretudo em face da LGPD, mediante a apresentação de propostas para a governança democrática. Outros temas a destacar foram os relacionados ao uso de tecnologias da informação e comunicação nos julgados, bem como de que forma os tribunais brasileiros estão empregando programas de inteligência artificial e como se poderia encontrar limites a essa utilização.

O primeiro a apresentar o trabalho foi o doutorando Ronaldo Felix Moreira Junior acerca da disseminação de notícias falsas e os limites do uso de dados pessoais em campanhas eleitorais, que abarcou a LGPD discutindo como os dados pessoais sensíveis têm sido empregados para fins políticos, como instrumentos de ataque à democracia. O discente Lorenzo Borges de Pietro apresentou o trabalho denominado "A (in) constitucionalidade da suspensão de plataformas da internet em decorrência do descumprimento de decisão judicial: um debate a luz do princípio da proporcionalidade, discutindo o alcance das decisões judiciais em termo de internet. O tema entabulado no próximo artigo foi o "Colonialismo Digital e os entraves à proteção de direitos fundamentais na era do Capitalismo de Vigilância", por Ronaldo Felix Moreira Junior, que apresentou o primeiro trabalho. Discutiu-se que os dados pessoais foram incluídos no rol de direitos fundamentais e que grandes empresas, contratadas para lidar com dados pessoais, podem empregá-los a seu talante. Portanto, deve existir uma tecnologia própria para a proteção deles. Pedro Ribeiro Fagundes apresentou o trabalho acerca da importância da gestão de riscos para a motivação dos atos administrativos. Esta motivação, essencial em todo o ato, deve levar em consideração os riscos que o gestor pode incidir, bem como os respectivos prejuízos que esses riscos podem produzir. Tainara Conti Peres e Deise Marcelino da Silva apresentaram o trabalho "A LGPD e a sua adequação no ambiente laboral: sob a ótica de controle do empregador privado brasileiro." As autoras inferem que a proteção de dados é própria desta época e abordaram, especificamente, as relações trabalhistas e analisam como se aplicam nas relações de trabalho, sobretudo sob a óptica do empregador privado. Valdir Rodrigues de Sá e Irineu

Francisco Barreto Júnior, que se encarregaram do tema “Liberdade de expressão nas plataformas digitais”, teve como objeto a análise da prática de crimes com a abertura da liberdade virtual existente no presente. O próximo trabalho apresentado por Gabrieli Santos Lacerda da Silva, dedicou-se ao tema “Os limites do consentimento frente ao direito fundamental de proteção dos dados pessoais”, que abordou a temática da mudança do comportamento humano diante dos avanços digitais. Nesse sentido, o grande volume de dados da internet, entre eles os dados pessoais, geram implicações na própria dinâmica social, o que fez a CF incluir dispositivos constitucionais e infraconstitucionais. Após a apresentação e aluna Tricieli Radaelli Fernandes e Fernando Hoffmam trouxeram a temática “O capital e a(s) guerra(s) na era do capitalismo de vigilância e a constituição de tecnopolíticas de combate”. O trabalho reflete que pode ser uma guerra real ou de violência simbólica diante da existência de tecnologias que podem perpetuar ou resgatar fórmulas capitalistas existentes nas diversas zonas. A seguir passou-se a apresentar por Estella Ananda Neves o artigo “Análise econômica do impacto da inteligência artificial nos tribunais brasileiros.” O baixo nível de investimentos e a parca participação de empresas brasileiras refletem o desenvolvimento atual do país e afirmam que o Judiciário pode em muito auxiliar o aprimoramento do Brasil. O primeiro bloco finalizou com a apresentação do trabalho “Administração Pública na era digital: uma análise sobre a segurança de dados nas sociedades de economia mista e empresas públicas à luz da LGPD” apresentado por Jean Marcel dos Santos. Como proteger os dados no atual panorama. O primeiro bloco foi encerrado com considerações dos coordenadores do GT, sobretudo o Prof. Galindo, que observou a questão da vigilância de dados nos sistemas jurídicos, a exemplo do que se pode observar na legislação europeia, como a que estabelece regras acerca da inteligência artificial, cuja matéria continua sendo regulada pelo Parlamento Europeu que, no último 14 de junho de 2023, aprovou sua posição negociadora sobre a Lei de Inteligencia Artificial. Importante recordar que esta norma incluí, entre os sistemas de alto risco os sistemas de IA que estão referidos na Administração de Justiça.

O segundo bloco de intervenções começou com o trabalho de Roseli Rêgo Santos Cunha Silva abordou no trabalho A LGPD e o tratamento de dados por agentes de pequeno porto: uma análise a partir da Resolução CD/ANPD N°2/2022. A abordagem indica que devem ser disponibilizados meios, compatíveis com as atividades de menor porte, considerando o bem que a LGPD objetiva proteger, a Resolução não exclui atores de menor porte; o discente Guilherme Elias Trevisan apresentou o trabalho “Big tech, dados, infraestruturas digitais e as universidades públicas federais brasileiras.” Restringiu-se a analise da verificação do sigilo da infraestrutura de dados e a disparidade de tecnologia que geram impactos geopolíticos, sobretudo nas universidades federais. Lidiana Costa de Sousa Trovão e Igor Marcellus Araujo Rosa apresentaram o trabalho intitulado “Cidades Inteligentes Sustentáveis,

governança e regulamentação de dados"; o trabalho analisa como essas cidades podem atingir o objetivo socioambiental e a quem são efetivamente destinadas. A seguir Luiz Fernando Mingati passou a expor o trabalho Constitucionalismo na era digital: os desafios impostos pela era informacional frente às garantias constitucionais. O artigo versa sobre como o impacto da era da informação e como ocorrem modificações na ordem interna geradas por esse fato. A seguir o Prof. Lucas Gonçalves da Silva apresentou juntamente com o aluno Reginaldo Felix "Tributação e Novas Tecnologias", os autores indicam que há uma tributação apresenta um novo percalço pela falta de transparência que os entes tributantes possuem diante desta atividade. O próximo trabalho trouxe a temática "Das cortes físicas às cortes digitais: a transformação digital dos tribunais como instrumento de acesso à justiça", pelo aluno Dennys Damião Rodrigues Albino; a temática se concentra na possibilidade de o Judiciário acompanhar a atual tendência digital e quais seriam as condicionantes a essas mudanças. A seguir David Elias Cardoso Camara apresentou o trabalho "Software de decisão automatizada como ferramenta de compliance no Tribunal de Justiça do Maranhão." O artigo estabelece uma análise geral sobre alguns documentos do Banco Mundial que analisa algumas ineficiências do Poder Judiciário. A seguir o aluno Pedro Gabriel C. Passos analisa no artigo "Desafios para concretização do ODS 8: análise a partir da dinâmica da indústria 4.0" que trata das TICs no ambiente do trabalho e alguns fenômenos que este pode apresentar em termos de prestação de serviços no mundo digital. Thiago Leandro Moreno seguiu apresentando o trabalho "Direito e Tecnologia: criptoativos e tokens não fungíveis", o trabalho versa sobre a ideia do metaverso e as transações ocorridas nos espaços virtuais. Novamente Irineu Francisco Barreto Jr e Kelly Cristina Maciel da Silva apresentaram o trabalho "O paradoxo entre a garantia constitucional do direito à informação e a preservação da privacidade em banco de dados públicos e privados." Constata-se pelo artigo que não existe ainda proteção suficiente para eventuais ataques virtuais.

O último bloco iniciou-se com o artigo "Mercosul X União Europeia: necessária adequação da autoridade nacional de proteção de dados" por Bruno Alexander Mauricio e Kennedy Josué Grecca de Mattos. A seguir apresentou-se o artigo "Mitigação de vieses algorítmicos em processos decisórios: os impactos da diversidade na constituição de equipes desenvolvedoras de inteligência artificial", por Airto Chaves Jr e Pollyanna Maria da Silva. O objetivo da investigação é verificar os impactos da constituição de equipes responsáveis pelas inteligências artificiais. Na sequencia José Octávio de Castro Melo apresentou o trabalho "Novas tecnologias e regulação: uma análise do PL 872/2021 face ao dever de diligência do Estado na proteção do direito à privacidade." A apresentação do trabalho "O uso da inteligência artificial no âmbito do processo judicial: desafios e oportunidades" por Jordy Arcadio Ramirez Trejo e Saulo Capelari Junior abordou de que forma deve ser implementada a inteligência artificial no âmbito do Poder Judiciário. A seguir Luciana

Cristina de Souza apresentou o trabalho “Risco no uso das inteligências artificiais e segurança digital” levando em consideração a atual forma que se aborda possíveis culpados com possível transgressão ao principio da presunção de inocência. Na sequência, Thais Aline Mazetto Corazza, expôs o trabalho “Os riscos na tomada de decisões por máquinas”. Já existe, no âmbito dos tribunais, certa triagem para evitar repetições e assim proporcionar melhores benefícios. Deve-se ter cuidado ao aplicar essas ferramentas, pois possuem subjetividades complexas. Bruno Mello Corrêa de Barros Beuron apresentou o trabalho “Revolução tecnológica e sociedade pós-moderna: perspectivas da obsolescência programada e do direito do consumidor à luz da metateoria do direito fraterno” . Luciana Rodrigues dos Santos e Aparecida Moreira de Oliveira Paiva apresentaram o artigo “Risco no uso das inteligências artificiais e segurança digital” em que se observa a questão relacionada a inteligência artificial pelos órgãos públicos e as questões discriminatórias.

Ao final houve manifestação de todos relativamente ao conteúdo apresentado e o quanto enriquecedor o Grupo de Trabalho foi para todos com ponderações extremamente profícuas de todos os presentes.

O PARADOXO ENTRE A GARANTIA CONSTITUCIONAL DO DIREITO À INFORMAÇÃO E A PRESERVAÇÃO DA PRIVACIDADE EM BANCO DE DADOS PÚBLICOS E PRIVADOS

THE PARADOX BETWEEN THE CONSTITUTIONAL GUARANTEE OF LAW TO INFORMATION AND THE PRESERVATION OF PRIVACY IN PUBLIC AND PRIVATE DATABASE

Kelly Cristina Maciel Da Silva Costa [1]
Irineu Francisco Barreto Junior [2]

Resumo

Este artigo irá correlacionar conceitos pertinentes ao Direito de Informação e de Privacidade de Dados com os da Ciência da Computação e da Engenharia da Informação, especialmente no ponto em que se confluem diante dos aspectos de segurança da informação. Para tanto, será realizada uma reflexão sobre a dinamicidade dos avanços das tecnologias em detrimento à adequação dos preceitos jurídicos, o que produz o excesso de liberalidade no metaverso em contraposição às problemáticas trazidas à privacidade. Concorrentemente, tendo em vista que a invasão e o sequestro de informações em Banco de Dados de Empresas Públicas e Privadas afetam com maior intensidade o interesse público, sobretudo por se tratar de uma coletividade de bens jurídicos afetados (pessoas físicas e jurídicas — públicas e privadas), será trazido neste artigo o conceito de Ransomwares — uma classe de Malwares que criptografa, ofusca e/ou impede o acesso ao banco de dados, promovendo o bloqueio de usuários — juntamente com o conceito e elucidação de algumas técnicas de Artificial Intelligence (AI) (Machine Learning (ML), Artificial Neural Networks (ANN) e Deep Learning) que visam prevenir e até mesmo detectar a origem dessas invasões, atuando conjuntamente com o Direito neste aspecto.

Palavras-chave: Liberalidade, Privacidade, Banco de dados, Rasomwares, Artificial intelligence

Abstract/Resumen/Résumé

This article will correlate concepts relevant to Information Law and Data Privacy with those of Computer Science and Information Engineering, especially at the point where they converge in the face of information security aspects. To this end, a reflection will be carried out on the dynamism of technological advances to the detriment of dependence on legal precepts, which produces excessive liberality in the metaverse in opposition to the problems

[1] Doutoranda e Mestra em Engenharia da Informação na UFABC. Bacharela em Engenharia Controle e Automação. Mestranda (FMU) e Bacharela em Direito (UNIP). Bacharelanda BC&T da UFABC. Professora universitária de Engenharia/Computação/TI.

[2] Pós Doutor em Sociologia pela USP. Doutor em Ciências Sociais PUC-SP. Professor do Programa de Mestrado em Direito da Sociedade da Informação FMU-SP. Analista de Pesquisas da Fundação Seade.

brought to privacy. At the same time, considering that the invasion and hijacking of information in the Database of Public and Private Companies killed the public interest with greater intensity, especially since it is a collective of judicial legal interests (individuals and legal entities - public and private), this article will bring the concept of Ransomware — a class of Malware that encrypts, obfuscates and/or prevents access to the database, blocking users — along with the concept and elucidation of some Artificial Intelligence (AI) techniques) (Machine Learning (ML), Artificial Neural Networks (ANN) and Deep Learning) that aim to prevent and even detect the origin of these invasions, coexisted together with the Law in this aspect.

Keywords/Palabras-claves/Mots-clés: Liberality, Privacy, Database, Rasomwares, Artificial intelligence

1 INTRODUÇÃO

O paradoxo entre o direito à informação e a privacidade nos bancos de dados, tanto públicos como privados, é um tema complexo e atual que tem sido objeto de discussão em diferentes esferas, incluindo a jurídica. De um lado, a Constituição Federal, em seu artigo 5º, inciso XIV, estabelece o direito de acesso à informação, que é um princípio fundamental da democracia, especialmente quando se trata de informações de interesse público. Por outro lado, o direito à privacidade, também previsto no artigo 5º, inciso X, é uma garantia fundamental e deve ser respeitado em todas as circunstâncias.

Nos bancos de dados públicos e privados, esses dois direitos muitas vezes se chocam, principalmente quando envolvem informações pessoais e sensíveis. Nesse sentido, a Lei Geral de Proteção de Dados (LGPD) estabelece normas para o tratamento de dados pessoais por entidades públicas e privadas. Além disso, a LGPD prevê a criação da Autoridade Nacional de Proteção de Dados (ANPD), que é responsável pela fiscalização e aplicação das normas previstas na lei. No entanto, a morosidade do Direito em relação às tecnologias de acesso a bancos de dados públicos e privados é uma questão relevante , especialmente no contexto de crescente digitalização da informação. A complexidade dos sistemas de tecnologia da informação e a rapidez com que as inovações ocorrem podem dificultar a aplicação eficaz do Direito.

Dentre os problemas sérios de invasões a banco de dados públicos e privados, os *Ransomwares* exigem uma atenção especial. Esses programas se infiltram nos sistemas de computador, criptografam os arquivos e exigem o pagamento de um resgate em troca da chave de descriptografia. Esse tipo específico de *Malware* é uma das principais ameaças à segurança dos bancos de dados, e podem causar diversos transtornos e prejuízos para empresas e organizações. Um dos casos mais notórios foi o ataque sofrido pela empresa Colonial Pipeline nos Estados Unidos em maio de 2021, que levou a uma paralisação da rede de oleodutos da empresa por dias e causou problemas de abastecimento em diversos estados norte-americanos. A empresa acabou pagando um resgate de cerca de US$ 4,4 milhões em bitcoin aos *hackers* (THE GUARDIAN, 2021). Outro exemplo foi o ataque sofrido pela empresa JBS, uma das maiores processadoras de carne do mundo, em maio de 2021. O ataque afetou as operações da empresa em diversos países, incluindo os Estados Unidos, e levou a uma interrupção temporária na produção. Embora a empresa não tenha revelado o valor do resgate pago aos hackers, relatos da imprensa indicam que o valor teria sido superior a US$ 11 milhões (BBC NEWS, 2021).

No Brasil, não existe uma lei específica que trate exclusivamente dos *Ransomwares*. Entretanto, a Lei nº 14.155/2021 prevê a tipificação do crime de invasão de dispositivo informático, incluindo a prática de criptografia indevida de dados. O artigo 154-A do Código Penal, incluído pela referida lei, define como crime "invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita".

No entanto, tendo em vista uma forma mais rápida de identificar e combater os ataques de *Ransomwares* há estudos que abordam a utilização de *Artificial Intelligence* (AI) — *Machine Learning*, *Deep Learning* e *Neural Networks* — (GHOSH, 2021), (MARSHALL, 2022), (IBM Security, 2018), (ALSHAMRANI; KHAN; ALGHATHBAR, 2019, p. 417-423), (RAJPUT; ANAND; BAJAJ, 2020, p. 38-43) como meio de preservação aos banco de dados. Concorrentemente, o relatório "*The State of Ransomware 2021*"da Sophos (SOPHOS, 2021) apresenta uma análise abrangente das tendências em invasões de *Ransomwares*, bem como o estudo em "*Artificial Intelligence for Cybersecurity Resilience*"da IBM (IBM Security, 2019), que explora as possibilidades de uso da AI para melhorar a segurança cibernética. Isso é devido ao fato dos sistemas de AI serem capazes de analisar grandes quantidades de dados e identificar comportamentos suspeitos em tempo real, permitindo uma resposta mais imediata a ameaças potenciais. Além disso, a AI pode melhorar a segurança dos bancos de dados, como por exemplo, na identificação de vulnerabilidades e na prevenção de ataques.

Portanto, é importante que os operadores do Direito entendam sobre os conceitos de AI, de banco de dados e de *Ransomwares*, uma vez que essas tecnologias estão cada vez mais presentes em nossas relações jurídicas. Compreender como funcionam e suas implicações contribui para que haja maior celeridade no embasamento de processos jurídicos circunstanciados, sobretudo devido ao maior conhecimento de causa.

1.1 Reflexão sobre o Acesso à Informação e a Invasão de Privacidade

O direito à informação e o direito à privacidade são direitos fundamentais previstos na Constituição Federal brasileira de 1988. O primeiro está disposto no artigo 5º, inciso XIV, que garante "acesso à informação"— algo essencial para a transparência e para o funcionamento democrático da sociedade. Já o segundo está previsto no artigo 5º, inciso X, que assegura

"a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas"— visa proteger a intimidade e a privacidade das pessoas.

Tendo em vista a abrangência do Direito à informação, previsto no art. 5º, XXXIII da CF, é importante analisar que há uma espécie de setorização e generalização acerca do seu conceito e abrangência, respectivamente, conforme dispõe a seguir Canotilho e Moreira (1993, p. 189).

> O direito à informação [...] integra três níveis: o direito de informar, o direito de se informar e o direito de ser informado. O primeiro consiste, desde logo, na liberdade de transmitir ou comunicar informações a outrem, de as difundir sem impedimentos, mas pode também revestir de forma positiva, enquanto direito a informar, ou seja, direito a meios para informar. O direito de se informar consiste designadamente na liberdade de recolha da informação, de procura de fontes de informação, isto é, no direito de não ser impedido de se informar. Finalmente, o direito de ser informado é a versão positiva do direito de se informar, consistindo num direito a ser mantido adequadamente e verdadeiramente informado, desde logo, pelos meios de comunicação [...] e pelos poderes públicos [...]

Paralelamente, Junior (2015, p. 57-71) conclui que o direito à informação é um conjunto de diretrizes legais subjetivas resultantes do preceito constitucional que tange sobre a liberdade de expressão.

1.1.1 *Contraposição entre o Direito à Informação e o Direito à Privacidade*

A tutela do Direito à Informação condiz com a liberalidade em promover acessos plurificados e incondicionados a bancos de dados variados. Devido a isso, este direito tem sido uma discussão latente em contraposição ao Direito à Privacidade, uma vez que atos decorrentes da violação deste se consubstanciam frequentemente em seus fundamentos. Portanto, os excessos cometidos que se embasam nessas prerrogativas ainda encontram imbróglios ao se caracterizarem na subsunção penal , e isso se dá pela dificuldade em se delinear ambos limites.

Juristas atuais têm discutido amplamente sobre este tema, como é o caso de Daniel Sarmento, professor de Direito Constitucional da UERJ, que destaca que o equilíbrio entre os direitos de informação e de privacidade deve ser buscado caso a caso, considerando as circunstâncias específicas de cada situação (SARMENTO, 2015, p. 405-434). Outro jurista importante que tem discutido esse tema é Ingo Sarlet, professor de Direito Constitucional da PUC-RS.

Em sua obra "Direitos Fundamentais e Relações Privadas", Sarlet destaca que a proteção da privacidade não pode ser vista como um obstáculo ao direito à informação, mas sim como um complemento necessário para que o direito à informação seja exercido de forma responsável e ética (SARLET, 2018, p. 35-36, 76-77).

Assegurar o acesso à informação está atrelado em garantir que todos acessem referências de qualidade e confiáveis, ao mesmo tempo em que se deve combater a disseminação de notícias falsas e promover a educação midiática para que as pessoas possam identificar e evitar a propagação de *fake news*. Um estudo feito por Massoni et al. (2022, p. 169-175) demonstra o paradoxo entre os limites da liberdade de expressão e do direito à informação, incluindo a análise das *fake news* — também denominadas como "desinformação"— que culminam no mau uso deste bem jurídico. Em seus estudos, Guilherme Bastos destaca a importância de se estabelecer limites à liberdade de expressão em casos de fake news, a fim de proteger a privacidade das pessoas envolvidas (BASTOS, 2019, p. 241-262). Marília Batista, por sua vez, discute os contornos e tensões entre os direitos fundamentais da privacidade, liberdade de expressão e acesso à informação, demonstrando como a disseminação de fake news pode prejudicar o exercício desses direitos (BATISTA, 2020, p. 129-150). Já Ronaldo Dias aborda a questão da privacidade e liberdade de expressão no combate às fake news, defendendo que é possível conciliar esses direitos fundamentais por meio de uma abordagem equilibrada e ponderada (DIAS, 2019, p. 105-130).

Assim, fica claro que o acesso à informação, juntamente com as temáticas que tangem sobre a privacidade, estão intimamente relacionadas, exigindo uma abordagem cuidadosa e fundamentada do ponto de vista jurídico, bem como a necessidade de um combate efetivo à desinformação produzida pela liberalidade nas redes.

2 OS AVANÇOS DA TECNOLOGIA E A PRIVACIDADE

Concorrente a circunstância jurídica de tutelas que tangem sobre direito da informação e do sigilo, não há como tratá-las sem levar em consideração que a tecnologia tem sido uma fonte propulsora, seja no cenário otimista ou pessimista. Neste tocante, o direito ao acesso à informação e o direito à privacidade ocupam espaços diametralmente opostos, separados por uma linha tênue. Segundo Moyses (2016, p. 4), as frentes ‘liberdade de expressão’, ‘privacidade’ e ‘acesso a conteúdos’ tem uma forte dependência, como também dispõe:

> No caso da liberdade de expressão, direito fundador das democracias modernas, são relatados casos de violações de diferentes naturezas[...] O tema da 'privacidade' também é abordado, e não à toa: a entrada de uma massa de milhões de pessoas no universo digital permitiu – e permite cada vez mais – o controle da vida dos indivíduos, de seus hábitos e de seus relacionamentos pessoais e sociais, propiciando a invasão da privacidade em diversos níveis [...]

Com o constante avanço da tecnologia, a invasão de privacidade tem se tornado uma questão cada vez mais preocupante. A coleta e o compartilhamento de dados pessoais sem o consentimento do indivíduo têm se tornado práticas comuns em diversas áreas, desde a publicidade online até a análise de dados em larga escala. Segundo Richards e King (2014, p. 229-243), a coleta de dados sem consentimento prévio pode ser considerada uma violação da privacidade, uma vez que o indivíduo tem o direito de decidir como suas informações serão utilizadas. A proteção da privacidade é um direito fundamental garantido por diversas legislações, como a *General Data Protection Regulation* (GDPR) na União Europeia e a Lei Geral de Proteção de Dados (LGPD) no Brasil.

Apesar dos avanços na legislação de proteção de dados, as práticas de invasão de privacidade continuam sendo uma realidade. Em seu estudo, Razaghpanah et al. (2021, p. 1-39) mostraram que diversas aplicações móveis coletam informações pessoais sem o conhecimento dos usuários, incluindo informações sobre sua localização e atividades online (RAZAGHPANAH et al., 2021). Outro ponto preocupante é a utilização de dados pessoais para fins de propaganda política e disseminação de fake news. Em seu estudo, Napoli destaca a importância de se garantir a privacidade dos indivíduos como forma de combater a desinformação online (NAPOLI, 2020).

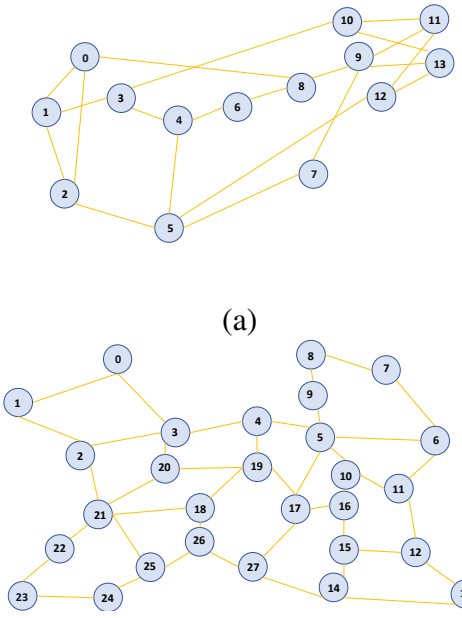
Diante desse cenário, é fundamental que sejam tomadas medidas efetivas para garantir a proteção da privacidade dos indivíduos. Além da criação de leis mais rigorosas e da fiscalização de práticas abusivas, é importante que os próprios usuários estejam cientes dos riscos e das práticas de proteção de dados, buscando utilizar serviços e aplicativos que respeitem sua privacidade.

2.1 Desigualdade de Acessos

Outra problemática nesta avalanche de acesso à informação é a questão de desigualdade. Ainda em Moyses (2016, p. 3), há uma reflexão acerca da relação entre a desigualdade

de acesso e formas de controle, onde aponta que é praticamente unânime a ideia da universalização da internet em contraposição à real possibilidade de todos usufruírem deste benefício. Inclusive, ainda segundo os seus estudos, locais no Brasil como a Amazônia e o bairro Paraisópolis em São Paulo, bem como em outros países como Quênia e bairros pobres de Detroit nos EUA, não detêm de infraestrutura de telecomunicações para a transmissão de internet. Já os estudos abordados em Costa, Nina e Bonani (2022)(i) e Nina, Costa e Bonani (2022)(ii) tratam exatamente de questões técnicas em redes ópticas elásticas — *Elastic Optical Networks* (EONs) —, especialmente sobre como promover melhor utilização dos recursos da rede diante da distribuição proporcional de rotas e de serviços, em que a população dos nós se torna uma variável importante de estudo sobre o seu desempenho, considerando assim, uma atuação realística de uma rede, visando otimizar o aproveitamento dos seus recursos (largura de banda) e evitar o não atendimento das requisições. As topologias da Figura 1 demonstram os grafos das redes consideradas, e a Tabela 1 demonstra as suas respectivas distribuições populacionais.

Figura 1: Redes de Internet Reais: (a) NFSNET, (b) PANEUR.



(a)

(b)
Fonte: Autor

A Figura 1(a) representa a topologia NSFNET (*National Science Foundation Network*), que é composta por 14 nós de borda interligados por 21 enlaces bidirecionais. A Figura 1(b) é a rede PANEUR (*Pan European*), que possui 28 nós de borda e, consequentemente, um número maior de enlaces. Na Tabela 1 é apresentada a quantidade populacional de cada nó das

respectivas redes e o local que estão concentrados. Para que haja maior entendimento sobre os conceitos técnicos relativos aos nós que compõem uma topologia, além da devida associação dos referidos termos à representatividade adequada, serão elucidados a seguir os dois tipos mais comuns de nós em uma rede:

- **nós de núcleo ou de passagem**: são os nós definidos exclusivamente para roteamento, não sendo origem nem destino de conexões;
- **nós de borda**: são os nós definidos prioritariamente como origem e destino de conexões, entretanto também exercendo a função de roteamento.

Tabela 1: Node Population Sizes for NSFNET and PANEUR Topologies

heightNode	**NSFNET**		**PANEUR**	
n	**City**	**Population**	**City**	**Population**
0	Seatle	776555	Glasgow	1680669
1	Palo Alto	63756	Dublin	1241953
2	San Diego	1427720	London	9425622
3	Salt Lake City	200831	Amsterdan	1157519
4	Boulder	105003	Hamburg	1788995
5	Houston	2323660	Berlin	3566791
6	Lincoln	293446	Warsaw	1789620
7	Atlanta	524067	Stockholm	1656571
8	Champaign	90739	Oslo	1056180
9	Pittsburg	299718	Copenhagen	1358608
10	Ann Arbor	329456	Prague	1312199
11	Ithaca	31193	Budapeste	1771865
12	College Park	32123	Belgrade	1401786
13	Princeton	31021	Athens	3153255
14			Rome	4278350
15			Zagreb	684524
16			Viena	1944910
17			Munich	1553373
18			Strasbourg	477978
19			Frankfurt	784780
20			Brussels	2095688
21			Paris	11078546
22			Bourdeaux	980130
23			Madrid	6668865
24			Barcelona	5624498
25			Lyon	1733581
26			Zurich	1407572
27			Milan	3144473

Vale salientar que a Tabela 1 traz uma expectativa de distribuição de rede de informação (internet), uma vez que é esperado que a quantidade populacional dos nós seja proporcional à quantidade de acessos. Essa hipótese não abrange necessariamente as questões sociais envolvidas que devem ser estudadas com profundidade, especialmente em países subdesenvolvidos onde se caracteriza uma alta desigualdade social. No entanto, como há uma variada complexidade de assuntos que estão associados à informação, sua disseminação e as suas devidas

consequências, este artigo ficará circunscrito em trazer algumas discussões que permeiam sobre a manutenção da privacidade nas redes diante da liberalidade contida no metaverso, tendo em vista algumas soluções imediatas que envolvem a utilização de AI para evitar invasões em banco de dados.

2.2 *Rasomwares*

Devido ao abrupto e contínuo avanço da tecnologia no âmbito cibernético, são realizados estudos constantes em busca de aperfeiçoar a segurança em sistemas de uso e armazenamento de dados contra a manipulação indevida de informações sigilosas. Os estudos abordados em Antoun e Malini (2011, p. 286-294), que tratam sobre a liberdade da rede e algumas problemáticas, mencionam sobre o ataque de hackers, que chegam a oferecer endereço de *proxy* via *direct message* no Twitter. Em grande parte dos casos, a maneira como se dá a inserção desses *hackers* em banco de dados, sobretudo empresariais, não é simples, requer habilidades e técnicas específicas, além de conhecimentos avançados sobre artifícios intermediadores indispensáveis como os *Ransomwares*. A invasão dessa classe de *Malwares* nos bancos de dados permite que haja o controle de acesso por criminosos, que visam negociar o restabelecimento do sistema mediante o pagamento de um "resgate"monetário.

Estudos demonstram que ataques de *Ransomwares* têm como alvo empresas e indústrias de sistemas de controle (ICS), e aumentou cerca de 500% do ano de 2018 a 2020 segundo Larson e Singleton (2020, p. 1-5). Ademais, de acordo com uma pesquisa realizada por Riskrecon (2021, p. 1307-1312), no período de um ano houve um aumento de 25 para 293 casos, de 2017 a 2021. Esses ataques afetam diretamente a operação de redes inteligentes, incluindo subestações (ALVEE et al., 2021, p. 1-5). Os efeitos produzidos pela criptografia e sequestro de dados têm gerado prejuízos financeiros absurdos. Segundo Ferreira (2017, p. 4-7), nos últimos anos muitas empresas no Brasil têm sido acometidas por muitos ataques desse tipo de vírus, paralisando as atividades e causando perdas gigantescas. Ainda, de acordo com as informações veiculadas no Jornal Folha de São Paulo (2018), as invasões de *ciberataques* a e-mails corporativos geram perdas de US$12,5 bilhões em cinco anos. A quantidade de empresas afetadas cresce continuamente, considerando estatisticamente apenas aquelas que divulgam os ataques, uma vez que nem todas disponibilizam essa informação por receio de um impacto negativo a sua imagem em relação à segurança dos dados. Nos EUA, ainda segundo Ferreira (2017, p. 5),

as empresas são obrigadas a divulgar ao público os incidentes relacionados à invasão virtual, facilitando com isso a apuração dos índices e, consequentemente, evidenciando a necessidade de mais pesquisas nesse âmbito.

Como menciona Ferreira (2017, p. 1), independentemente do sistema operacional (Android, iOS, Windows), os riscos impostos por esse tipo de exploração de falhas por meio de *Ransomware* são relevantes. Os métodos de detecção de *Ransomwares* são classificados em duas categorias: métodos de análise estática e métodos de análise dinâmica (ALVEE et al., 2021, p. 1). Embora os métodos de análise estática sejam mais simples para a detecção e implementação (AHN et al., 2021, p. 1307-1312) (pelo fato de usarem dados estásticos), eles são amplamente ineficazes contra ataques de *Ramsonwares* mais avançados (KHARRAZ et al., 2015, p. 3-24). Tendo isso em vista, em Poudyal e Dasgupta (2020) há a abordagem sobre a combinação de ambos os métodos (estático e dinâmico) para potencializar a eficiência na detecção destes *Malwares*.

Esta problemática implica em analisar as formas de garantir o direito constitucional de acesso à informação de forma irrestrita, incondicionada e ilimitada, mas preservando aquelas que são tuteladas pelo direito à privacidade. No que tange à última, o cenário tem ficado cada vez mais preocupante, sobretudo porque o metaverso oferece inúmeras ferramentas de acesso à informação sem o proporcional controle disso, ocasionando uma diversidade de problemas resultantes do mal uso dessas atribuições por entes com fins dolosos. Uma forma de assegurar a privacidade diante da liberdade nas redes é buscar meios imediatistas de combater invasões de forma proporcional, uma vez que as leis ainda são morosas neste sentido. Tendo em vista os avanços da Inteligência Artificial, este artigo busca reunir o meio jurídico e computacional, com o fim de confluir alguns interesses pontuais para melhorar o convívio da sociedade nas redes.

Não é novidade a busca por mais segurança na preservação de dados empresarias de âmbito público e privado, e atualmente a AI tem sido uma ferramenta de pesquisa para a implementação de medidas de maior confiabilidade e mais eficiência no combate contra invasões, inclusive em Khammas (2020, p. 325-331) já foi abordado o uso dessa técnica para melhorar a precisão em análise estática. Nas pesquisas realizadas em Alvee et al. (2021, p. 1-5), Agrawal et al. (2019, 3222-3226) e Adamov e Carlsson (2020, p. 1-5), houve a utilização de *Convolutional Neural Network* (CNN) (com 96.22% de precisão), de *Recurrent Neural Networks* (RNN) e de *Reinforcement Learning* (RL), respectivamente, para a detecção de ataques de *Ransomwares*.

Em Cusack, Michel e Keller (2018, p. 1-6) utilizaram dados de uma rede para aplicar *Machine Learning* (ML) e *Random Forest* (RF) na detecção de *Ransomwares* e obtiveram mais 86% de precisão na detecção. Ainda, em Veeramachaneni et al. (2016, p. 49-54) e Chu e Song (2021, p. 390-393) há a combinação de técnicas como *Internet of Things* (IOT) e *Analyst Intuition* (AIn) com AI, além de Maimó et al. (2019, p. 1-31) apresentar a combinação entre ML, *Navie Bayes* (NB) e *Support Vector Machine* (SVM), com uma precisão de 99.99% na detecção. Há também alguns estudos sobre a segurança de métodos de detecção de *Ramsonwares* utilizando AI, como o desenvolvido em Tao e Zhang (2021, p. 102-105).

2.3 Noções Básicas de *Machine Learning* aplicada em Banco de Dados

A técnica de Aprendizagem de Máquina (*Machine Learning*) é um segmento da Inteligência Artificial (IA) que permite que um sistema computacional possa aprender a partir de um banco de dados, definindo padrões estatisticamente estabelecidos para a definição de uma classe (resultado). Esse tipo de sistema é treinado usando um grande volume de dados que, às suas vezes, necessitam de alguns tratamentos específicos, algo denominado na literatura como mineração de dados. A mineração de dados (ou data mining) é o processo de explorar grandes quantidades de dados para descobrir padrões, tendências e informações úteis que possam ser usadas para tomar decisões pré-estabelecidas, desprezando aqueles dados que não são interessantes para a extração de determinada informação. Envolve a utilização de técnicas estatísticas e análises gráficas para a extração de informações significativas a partir de grandes conjuntos de dados estruturados ou não estruturados.

Existem basicamente três tipos principais de técnicas de *Machine Learning*: supervisionado, não supervisionado e por reforço. O aprendizado supervisionado envolve o treinamento do sistema com dados rotulados (resultados prévios de alguns elementos do banco de dados), ou seja, dados que já foram classificados por um humano, para que o sistema possa aprender a identificar padrões e classificar novos dados. O aprendizado não supervisionado, por sua vez, é usado para identificar padrões em conjuntos de dados não rotulados, enquanto o aprendizado por reforço é usado para treinar sistemas para tomar decisões baseadas em *feedback* de recompensa ou penalidade.

O Machine Learning é amplamente utilizado em diversas áreas, como reconhecimento de voz, detecção de fraudes, diagnósticos, análise de sentimentos em redes sociais, entre outros.

A utilização desta técnica em bases de dados jurídicos tem ganhado cada vez mais destaque, principalmente na área de análise preditiva e de tomada de decisão. Algumas possíveis aplicações incluem a análise de sentenças judiciais para identificar padrões e tendências. Um exemplo de pesquisa nesse sentido é o artigo "Machine Learning and the Law: Predictive Analytics for Law and Policy", de Daniel Katz, Michael Bommarito II e Josh Blackman (KATZ; II; BLACKMAN, 2017, p. 13-24). Outra aplicação interessante é em análise de contratos para identificar cláusulas problemáticas, como cláusulas que violam leis de defesa do consumidor ou cláusulas que podem gerar litígios no futuro. Um exemplo de pesquisa nesse sentido é o artigo "Artificial Intelligence and Contract Law: Delivering on the Promise of Big Data Analysis", de Ian Kerr, David Wishart e Alexandre Skander Galand (KERR; WISHART; GALAND, 2018, p. 353-396). Mais correlacionado ao assunto de invasão de privacidade, há a aplicação na detecção de fraudes. Isso pode incluir a análise de transações financeiras, a análise de dados de clientes e a análise de dados de fornecedores. Essa análise pode ajudar a identificar possíveis fraudes antes que elas ocorram e a tomar medidas preventivas. Um exemplo de pesquisa nesse sentido é o artigo "Using Machine Learning Techniques to Detect Fraud in Healthcare Claims", de Jean-Luc Bouchard e Melissa M. Smith (BOUCHARD; SMITH, 2019, p. 21-32).

Os códigos de *Machine Learning* possuem estratégias diferentes e as respectivas aplicações podem variar de acordo com as necessidades envolvidas. Dentre os existentes, serão listados pelo menos 5 exemplos de algoritmos que possuem código aberto (livre acesso):

- Random Forest: o Random Forest é um algoritmo de aprendizado supervisionado que utiliza árvores de decisão para realizar a classificação ou regressão. Ele é considerado um dos algoritmos mais poderosos e flexíveis, capaz de lidar com dados não lineares e heterogêneos. A implementação em Python (linguagem de programação) está disponível no pacote scikit-learn (biblioteca);

- Naive Bayes: Naive Bayes é um algoritmo de aprendizado supervisionado que é frequentemente utilizado para classificação de texto, análise de sentimentos e filtragem de spam. Ele é baseado no Teorema de Bayes e assume que as características são independentes entre si. O Naive Bayes é considerado um algoritmo simples, mas eficiente. A implementação em Python também está disponível no pacote scikit-learn;

- Support Vector Machines (SVM): O SVM é um algoritmo de aprendizado supervisionado que é frequentemente utilizado para classificação e regressão. Ele é capaz de lidar

com dados de alta dimensão e separáveis linearmente ou não linearmente. O SVM é considerado um dos algoritmos mais precisos, mas também pode ser computacionalmente intensivo. A implementação em Python está disponível no pacote scikit-learn;

- K-Means: O K-Means é um algoritmo de aprendizado não supervisionado que é frequentemente utilizado para clustering ou agrupamento de dados. Ele divide um conjunto de dados em K clusters (conjuntos de amostras), onde K é o número de clusters desejado. O K-Means é considerado um algoritmo simples e eficiente. A implementação em Python também está disponível no pacote scikit-learn;

- Gradient Boosting: O Gradient Boosting é um algoritmo de aprendizado supervisionado que é frequentemente utilizado para classificação ou regressão. Ele constrói um conjunto de modelos de aprendizado fraco e combina-os para produzir um modelo forte. O Gradient Boosting é considerado um dos algoritmos mais poderosos, mas também pode ser computacionalmente intensivo. A implementação em Python está disponível no pacote scikit-learn.

Esses algoritmos são amplamente utilizados em várias áreas de aplicação de machine learning e possuem implementações de código aberto em Python, o que torna fácil para os usuários utilizá-los em seus projetos de machine learning.

2.3.1 *Etapas de Mineração de Banco de Dados*

Tendo em vista que o desempenho dos algoritmos de *Machine Learning* possui forte dependência em relação à qualidade dos dados disponíveis (informação disponível para o modelo aprender), se faz necessário algumas etapas de extração, pré-processamento e análise de banco de dados. Essas fases são imprescindíveis para otimizar os resultados da aplicação de *Machine Learning*, conforme abordado em Jain et al. (2020, p. 3561-3562). Os atributos de um banco de dados são os elementos identificadores das entidades existentes no banco de dados e podem ser classificados de acordo com seu tipo, escala, representação numérica e descrição, de maneira que seja possível entender quais modelos de classificação podem ser mais adequados para futura implementação. Além disso, o uso da estatística descritiva nos atributos, o cálculo da correlação e do modelo regressão linear, juntamente com as respectivas representações gráficas, têm como objetivo representar a distribuição dos dados e identificar a existência de *ou-*

tliers e de inconsistências (ruídos) que podem comprometer significativamente o desempenho do algoritmo de classificação.

Apenas para demonstrar algumas etapas estatísticas importantes e as suas respectivas informações extraídas para a aplicação de aprendizado de máquina supervisionado, será utilizado como exemplo o resultado de um tratamento realizado pelos autores deste artigo no banco de dados clínicos da *Heart Disease Data Set* da Fundação da Clínica Cleveland *(*Cleveland Clinic Foundation) (DETRANO M.D.,).

O *Heart Disease Data Set* contém 303 amostras de dados e 14 atributos. Sucintamente, o primeiro passo ao analisar banco de dados é classificar quais os tipos de atributos, se são qualitativos (na maior parte das vezes são elementos não numéricos como cor, idade, tamanho, sexo etc) e quantitativos (são eminentemente numéricos, como idade, nível de colesterol, temperatura, pressão etc). Na Tabela 2 são apresentados 6 quantitativos (’age’ - idade, ’trestbps’ - pressão arterial em repouso, ’chol’ - nível de colesterol, ’thalach’ - frequência cardíaca máxima alcançada, ’oldpeak’ - depressão de ST induzida por exercício em relação ao repouso, ’ca’ - número de vasos principais (0-3) coloridos por fluoroscopia) e o resultado dos cálculos estatísticos como média, moda, mediana, variância, desvio padrão aplicados nas 303 amostras, conforme demonstrado abaixo.

Tabela 2: Estatística Descritiva

Atributos	Mínimo	Máximo	Média	Desvio Padrão	Variância	Moda
age	29,00	77,00	54.542088	9.049736	81.897716	58.0
trestbps	94.0	200.0	131.693603	17.762806	315.517290	120.0
chol	126.0	564.0	247.350168	51.997583	2703.748589	197.0
thalach	71.0	202.0	149.599327	22.941562	526.315270	162.0
oldpeak	0.0	6.2	1.055556	1.166123	1.359842	0.0
ca	0.0	3.0	0.676768	0.938965	0.881654	0.0

Já na Tabela 3 são apresentados os 8 atributos qualitativos (’sex’ - sexo, ’cp’- tipo de dor no peito, ’fbs’ - nível de açúcar no sangue em jejum, ’restecg’ - resultados eletrocardiográficos em repouso, ’exang’ - angina induzida por exercício, ’slope’ - a inclinação do pico do segmento ST do exercício, ’thal’ - nível de normalidade, ’num’ - diagnóstico de doença cardíaca, atributo alvo), existentes no banco de dados estudado.

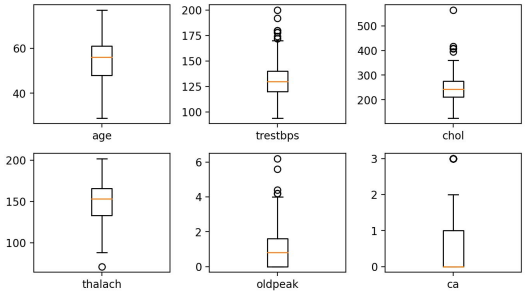
Tabela 3: Atributos Qualitativos

Atributos	Escala	Representação Numérica	Descrição
sex	Nominal	0/1	1-homem, 0-mulher
cp	Nominal	1/2/3/4	Tipo de dor no peito: 1-típica, 2-atípica, 3- não anginoso pain,4- assintomático
restecg	Nominal	0/1/2	0-normal, 1-anormalidade da onda ST-T, 2-hipertrofia ventricular esquerda
exang	Nominal	0/1	Angina induzida por exercício (sim ou não)
slope	Ordinal	1/2/3	Inclinação do pico do segmento ST do exercício (ascendente, plana ou descendente)
thal	Nominal	3/6/7	3 = normal; 6 = fixed defect; 7 = reversable defect
fbs	Ordinal	0/1	(fasting blood sugar > 120 mg/dl) (1 = true; 0 = false)
num	Nominal	0/1/2/3/4	0==0 (não doente), 1/2/3/4==1(doente)

Com os dados estatísticos são gerados gráficos como os da Figura 2, 3, 4, 5 que representam informações sobre a distribuição dos dados para os atributos quantitativos e qualitativos apresentados nas Tabelas 2 e 3.

O Boxplot (também conhecido como diagrama de caixa) apresentado na Figura 2 é uma ferramenta gráfica usada para representar a distribuição de um conjunto de dados. É especialmente útil para identificar *outliers* (valores extremos) e para comparar a distribuição de um conjunto de dados com outro. É composto por um retângulo que representa o intervalo interquartil (IQR), que contém 50% dos dados. A mediana é representada por uma linha dentro do retângulo. As extremidades superiores e inferiores do retângulo representam o terceiro quartil (Q3) e o primeiro quartil (Q1), respectivamente. Além do retângulo, há linhas chamadas de bigodes, que representam a amplitude dos dados. Os bigodes são geralmente definidos como o menor valor dentro de 1,5 vezes o IQR abaixo do Q1 e o maior valor dentro de 1,5 vezes o IQR acima do Q3. Os *outliers* são representados por pontos individuais acima ou abaixo dos bigodes.

Figura 2: Boxplot dos Atributos Quantitativos

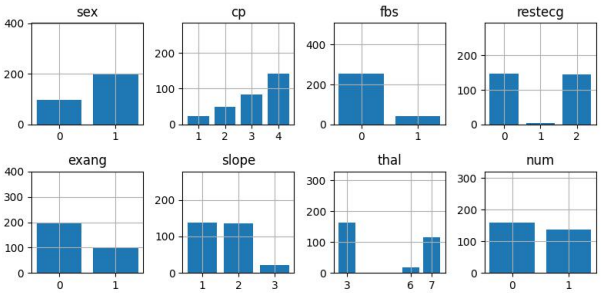


Fonte: Autor

Portanto, verifica-se possíveis valores *outliers* nos atributos ca, oldpeak, chol e trestbps, acima de 1.5 vezes o intervalo interquartil.

O Histograma, apresentado na Figura 3 é um gráfico utilizado na estatística para representar a distribuição de frequência de um conjunto de dados contínuos. Ele consiste em um conjunto de retângulos adjacentes, cujas alturas correspondem às frequências observadas em cada intervalo de classe dos dados. Para construir um histograma, o intervalo de valores dos dados é dividido em um conjunto de classes e a frequência de ocorrência de cada classe é contada. Cada classe é representada por um retângulo com base na largura da classe e com altura correspondente à frequência. O resultado é um gráfico em que a área de cada retângulo representa a frequência da classe correspondente.

Figura 3: Histograma dos Atributos Qualitativos



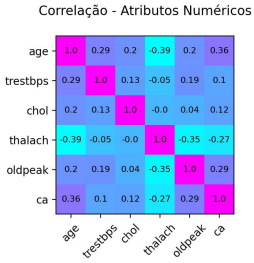
Fonte: Autor

Portanto, os histogramas apresentados indicam o número de ocorrências de cada categoria no *dataset*, onde se constata, por exemplo, que aproximadamente 2/3 das observações são de homens.

A Correlação entre as variáveis estatísticas, como demonstra o gráfico da Figura 4,

serve para avaliar a relação linear entre duas variáveis quantitativas. Ela é utilizada para entender como as variáveis estão relacionadas entre si e pode ajudar a identificar possíveis padrões ou tendências nos dados. A correlação é expressa em um coeficiente que varia de -1 a 1, onde valores próximos de -1 indicam uma correlação negativa forte, valores próximos de 1 indicam uma correlação positiva forte e valores próximos de 0 indicam ausência de correlação linear.

Figura 4: Correlação Entre os Atributos



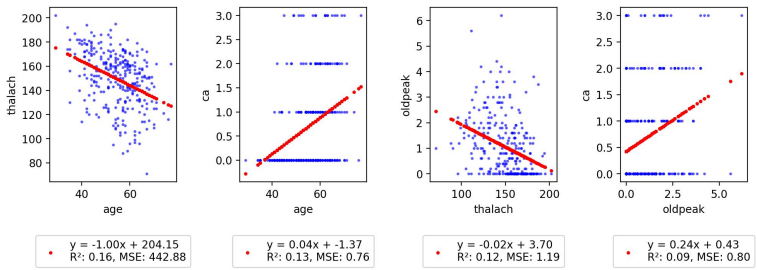
Fonte: Autor

É importante salientar que a diagonal da matriz de correlação sempre será composta somente pelo número 1, uma vez que representa a correlação das variáveis com elas próprias, obviamente trazendo uma correlação de 100%.

A Regressão linear é um tipo de gráfico usado em estatística para visualizar a relação entre duas variáveis quantitativas, uma variável é considerada independente (ou explicativa) e a outra é a dependente (ou resposta), conforme demonstra a Figura 5. A linha de regressão é a linha reta que melhor se ajusta aos dados, ou seja, é a linha que minimiza a soma dos quadrados das distâncias entre os pontos observados e a linha. O objetivo principal do gráfico de regressão é determinar se há uma relação linear entre as duas variáveis e, em caso afirmativo, avaliar a força e a direção dessa relação. Valores próximos a 1 indicam uma relação forte e positiva, valores próximos a -1 indicam uma relação forte e negativa e valores próximos a 0 indicam pouca ou nenhuma relação linear. O gráfico de regressão também pode ser usado para fazer previsões ou estimativas da variável dependente para valores específicos da variável independente que não foram observados. A partir dos resultados de regressão (Figura 5) é observado uma dependência linear negativa entre a idade (age) e o número máximo de batimentos do coração (thalach), e entre este atributo em relação à depressão de ST induzida por exercício em relação ao repouso (oldpeak), onde é possível concluir uma relação de causalidade nos valores previstos segundo o modelo. Já para a regressão que contém o atributo ca (número de vasos principais coloridos por fluoroscopia) em relação ao oldpeak e ao atributo age é necessário um maior conhecimento

para interpretar o comportamento do respectivo gráfico.

Figura 5: Regressão dos Atributos Quantitativos



Fonte: Autor

3 CONCLUSÃO

Tendo em vista a liberalidade existente nas redes, que se explicita de forma indiscriminada e incondicionada, sobretudo pelas prerrogativas que se alicerçam no Direito à Informação, há invariavelmente maior suscetibilidade de atividades peremptoriamente dolosas, como as promovidas por *Ransomwares*. Portanto, este artigo demonstrou a interconexão entre o conhecimento jurídico e computacional no que diz respeito à informação e aos avanços da tecnologia no metaverso. O conceito e a aplicação de AI, especificamente de *Machine Learning*, foi elucidada como uma solução imediata para evitar ações dolosas, juntamente com a elucidação de outras estratégias como *Deep Learning* e *Neural Networks*. Portanto, os estudos aqui trazidos desmistificaram as diferenças impostas entre as ciências sociais e exatas, demonstrando que podem atuar conjuntamente para um propósito comum.

Referências

ADAMOV, A.; CARLSSON, A. **Reinforcement Learning For Anti-Ransomware Testing**. In: *2020 Ieee East-West Design And Test Symposium (Ewdts)*. [S.l.: s.n.], 2020. p. 1–5.

AGRAWAL, R. et al. **Attention In Recurrent Neural Networks For Ransomware Detection**. In: *Icassp 2019 - 2019 Ieee International Conference On Acoustics, Speech And Signal Processing (Icassp)*. [S.l.: s.n.], 2019. p. 3222–3226.

AHN, B. et al. **Blockchain-Enabled Security Module For Transforming Conventional Inverters Toward Firmware Security-Enhanced Smart Inverters**. In: *2021 Ieee Energy Conversion Congress And Exposition (Ecce)*. [S.l.: s.n.], 2021. p. 1307–1312.

ALSHAMRANI, A.; KHAN, A.; ALGHATHBAR, K. **Ransomware Detection using Machine Learning Techniques: A Review**. *International Journal of Advanced Computer*

Science and Applications, v. 10, n. 9, p. 417–423, 2019. Disponível em: https://doi.org/10.14569/IJACSA.2019.0100947. Acesso em 05 de abril de 2023.

ALVEE, S. R. B. et al. **Ransomware Attack Modeling And Artificial Intelligence-Based Ransomware Detection For Digital Substations**. In: *2021 6th Ieee Workshop On The Electronic Grid (Egrid)*. [S.l.: s.n.], 2021. p. 01–05.

ANTOUN, H.; MALINI, F. **Ontologia Da Liberdade Na Rede: A Guerra Das Narrativas Na Internet E A Luta Social Na Democracia** . *Revista Famecos*, v. 17, n. 3, p. 286–294, 2011. Disponível em: https://revistaseletronicas.pucrs.br/ojs/index.php/revistafamecos/article/view/8196/5885. Acesso em 05 de abril de 2023.

BASTOS, G. M. M. **Privacidade e direito à informação: limites à liberdade de expressão em tempos de fake news**. *Revista de Informação Legislativa*, Senado Federal, v. 56, n. 222, p. 241–262, 2019.

BATISTA, M. F. **Fake news, privacidade e liberdade de expressão: contornos e tensões entre direitos fundamentais na sociedade da informação**. In: *Direito e Novas Tecnologias*. [S.l.]: D'Plácido, 2020. p. 129–150.

BBC NEWS. **JBS: Cyber-attack hits world's largest meat supplier**. v. 17, n. 3, p. 286–294, 2021. Disponível em: https://www.bbc.com/news/world-us-canada-57318965. Acesso em 08 de abril de 2023.

BOUCHARD, J.-L.; SMITH, M. M. **using machine learning techniques to detect fraud in healthcare claims**. *Journal of Health Care Finance*, v. 45, n. 2, p. 21–32, 2019.

CANOTILHO, J. J. G.; MOREIRA, V. **Constituição Da República Portuguesa Anotada**. [S.l.: s.n.], 1993. 189 p.

CHU, M.; SONG, Y. **Analysis Of Network Security And Privacy Security Based On Ai In Iot Environment**. In: *2021 Ieee 4th International Conference On Information Systems And Computer Aided Education (Iciscae)*. [S.l.: s.n.], 2021. p. 390–393.

COSTA, K. C. M. S.; NINA, F. D.; BONANI, L. H. **Routing Traffic Distribution And The Performance Correspondence For Optical Networks**. p. 5, 2022. Disponível em: https://doi.org/10.1109/SBFotonIOPC54450.2022.9992889. Acesso em 08 de abril de 2023.

CUSACK, G.; MICHEL, O.; KELLER, E. **Machine Learning-Based Detection Of Ransomware Using Sdn**. In: . New York, Ny, Usa: Association For Computing Machinery, 2018. (Sdn-Nfv Sec'18), p. 1–6. ISBN 9781450356350. Disponível em: https://doi.org/10.1145/3180465.3180467. Acesso em 07 de abril de 2023.

DETRANO M.D., P. C. C. F. R. **Heart Disease Data Set**, year = 1998, address= Dragos, White Paper, month = July,. In: . [S.l.: s.n.].

DIAS, R. B. d. C. **Direito à privacidade e liberdade de expressão no combate às fake news**. In: OLIVEIRA, M. A. C. d.; MOURA, M. T. R. d. A. (Ed.). *Direito, democracia e fake news*. [S.l.]: Arraes, 2019. p. 105–130.

FERREIRA, L. M. **Os Riscos Do Sequestro De Informações Pelos Ransowares**. Dissertação (Mestrado) — Universidade Do Sul De Santa Catarina - Unisul, May. 2017.

GHOSH, P. **Using Artificial Intelligence to combat the growing threat**. *Forbes*, 2021. Disponível em: https://www.forbes.com/sites/forbestechcouncil/2021/06/25/ransomware-using-artificial-intelligence-to-combat-the-growing-threat/?sh=7fcb9e9a1010. Acesso em 08 de abril de 2023.

IBM Security. **Using Artificial Intelligence to Fight Ransomware**. *IBM Security Intelligence*, 2018. Disponível em: https://www.ibm.com/security/data-breach/artificial-intelligence-ransomware. Acesso em 02 de março de 2023.

IBM Security. **Artificial Intelligence for Cybersecurity Resilience**. 2019. Disponível em: https://www.ibm.com/security/data-breach/intelligence/ai-cybersecurity-resilience. Acesso em 08 de abril de 2023.

JAIN, A. et al. **Overview And Importance Of Data Quality For Machine Learning Tasks**. In: *Proceedings Of The 26th Acm Sigkdd International Conference On Knowledge Discovery & Data Mining*. [S.l.: s.n.], 2020. p. 3561–3562.

Jornal Folha de São Paulo. **Novas Armas Dos Eua Vulneráveis A Ciberataques, Aponta Relatório**. Dragos, White Paper: [s.n.], 2018.

JUNIOR, J. F. D. M. **O Direito à Informação e o Acesso A Documentos Públicos Da Ditadura Militar: A Proteção Pela Jurisdição Constitucional**. *Interfaces Científicas - Direito*, v. 3, n. 2, p. 57–71, Mar. 2015. Disponível em: https://doi.org/10.17564/2316-381x.2015v3n2p57-71. Acesso em 08 de abril de 2023.

KATZ, D. M.; II, M. J. B.; BLACKMAN, J. **Machine Learning and the Law: Predictive Analytics for Law and Policy**. [S.l.]: Edward Elgar Publishing, 2017.

KERR, I.; WISHART, D.; GALAND, A. S. **Artificial Intelligence and Contract Law: Delivering on the Promise of Big Data Analysis**. *Ottawa Law Review*, v. 49, n. 2, p. 353–396, 2018.

KHAMMAS, B. M. **Ransomware Detection Using Random Forest Technique**. In: . [S.l.: s.n.], 2020. v. 6, n. 4, p. 325–331. ISSN 2405-9595. Disponível em: https://doi.org/10.1016/J.Icte.2020.11.001. Acesso em 05 de abril de 2023.

KHARRAZ, A. et al. **Cutting The Gordian Knot: A Look Under The Hood Of Ransomware Attacks**. In: . [S.l.: s.n.], 2015. p. 3–24. ISBN 978-3-319-20549-6.

LARSON, S.; SINGLETON, C. **Ransomware In Ics Environments**. In: *2021 6th Ieee Workshop On The Electronic Grid (Egrid)*. [S.l.: s.n.], 2020. p. 01–05.

MAIMó, L. F. et al. **Intelligent And Dynamic Ransomware Spread Detection And Mitigation In Integrated Clinical Environments**. *Sensors*, v. 19, n. 5, 2019. ISSN 1424-8220. Disponível em: https://www.mdpi.com/1424-8220/19/5/1114. Acesso em 04 de abril de 2023.

MARSHALL, D. W. **Ransomware: How AI is helping to fight this cyber menace**. *TechRepublic*, 2022. Disponível em: https://www.techrepublic.com/article/ransomware-how-ai-is-helping-to-fight-this-cyber-menace/. Acesso em 01 de março de 2023.

MASSONI, L. F. H. et al. **A Sociedade Do Espetáculo E As Fake News: Provocações E Implicações Perante O Direito À Informação**. *Biblos*, v. 36, n. 1, Set. 2022. Disponível em: https://periodicos.furg.br/biblos/article/view/13420/9858. Acesso em 10 de abril de 2023.

MOYSES, D. **Freenet: Direitos E Liberdade Na Internet**. *Revista Eletrônica De Comunicação, Informação Amp; Inovação Em Saúde*, v. 10, n. 3, Set. 2016. Disponível em: https://www.reciis.icict.fiocruz.br/index.php/reciis/article/view/1190. Acesso em 15 de abril de 2023.

NINA, F. D.; COSTA, K. C. M. S.; BONANI, L. H. **Performance Evaluation Of Elastic Optical Networks Under Scenarios With Unequal Distribution Of Service Types Per Route Length**. p. 5, 2022. Disponível em: https://doi.org/10.1109/Sbfotoniopc54450.2022.9992530. Acesso em 08 de abril de 2023.

POUDYAL, S.; DASGUPTA, D. Ai-powered ransomware detection framework. In: *2020 Ieee Symposium Series On Computational Intelligence (Ssci)*. [S.l.: s.n.], 2020. p. 1154–1161.

RAJPUT, S.; ANAND, D.; BAJAJ, P. **Using Machine Learning to Detect Ransomware Attacks on Cloud Storage Services**. In: *2020 International Conference on Information Technology (ICIT)*. [S.l.: s.n.], 2020. p. 38–43.

RAZAGHPANAH, A. et al. **Privacy Challenges in Mobile and Web Application Development**. *ACM Computing Surveys*, v. 54, n. 4, 2021.

RICHARDS, N. M.; KING, J. H. **Three paradoxes of Big Data**. *Stanford Law Review*, v. 66, n. 2, p. 229–243, 2014.

RISKRECON. **Five Lessons Learned From Over 600 Ransomware Attacks**. In: *Ransomware Attacks*. [S.l.: s.n.], 2021.

SARLET, I. W. **Direitos Fundamentais e Relações Privadas**. [S.l.]: Livraria do Advogado Editora, 2018.

SARMENTO, D. **A ponderação de interesses na jurisprudência do STF**. *Revista Direito GV*, FGV Direito SP, v. 11, n. 2, p. 405–434, 2015.

SOPHOS. **The State of Ransomware 2021**. 2021. Disponível em: https://news.sophos.com/en-us/2021/04/27/the-state-of-ransomware-2021/. Acesso em 8 de abril de 2023.

TAO, X.; ZHANG, H. **Research On Data Security Governance Based On Artificial Intelligence Technology**. In: *2021 International Conference On Big Data, Artificial Intelligence And Risk Management (Icbar)*. [S.l.: s.n.], 2021. p. 102–105.

THE GUARDIAN. **Hacked US energy pipeline on track to restore full service but shortages persist**. 2021. Disponível em: https://www.theguardian.com/us-news/2021/may/15/us-energy-pipeline-colonial-ransomware-attack. Acesso em 8 de abril de 2023.

VEERAMACHANENI, K. et al. **AI: Training A Big Data Machine To Defend**. In: *2016 Ieee 2nd International Conference On Big Data Security On Cloud (Bigdatasecurity)*. [S.l.: s.n.], 2016. p. 49–54.