XIII ENCONTRO INTERNACIONAL DO CONPEDI URUGUAI – MONTEVIDÉU

GOVERNO DIGITAL, DIREITO E NOVAS TECNOLOGIAS I

DANIELLE JACON AYRES PINTO

YURI NATHAN DA COSTA LANNES

LAURA INÉS NAHABETIÁN BRUNET

Copyright © 2024 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria – CONPEDI
Presidente - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - FMU – São Paulo
Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC – Santa Catarina
Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa – Pará
Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG – Goiás
Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos – Rio Grande do Sul
Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio – Rio de Janeiro
Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:
Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão
Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais
Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte
Prof. Dr. Fernando Passos – UNIARA - São Paulo
Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP - São Paulo
Secretarias
Relações Institucionais:
Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná
Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia
Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal
Comunicação:
Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina
Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul
Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe
Relações Internacionais para o Continente Americano:
Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do Sul
Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão
Prof. Dr. Felipe Chiarello de Souza Pinto - UPM – São Paulo
Relações Internacionais para os demais Continentes:
Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará
Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul
Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI – Santa Catarina
Eventos:
Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo
Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina
Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Membro Nato – Presidência anterior Prof. Dr. Raymundo Juliano Feitosa – UNICAP – Pernambuco

D597

GOVERNO DIGITAL, DIREITO E NOVAS TECNOLOGIAS I

[Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Danielle Jacon Ayres Pinto, Yuri Nathan da Costa Lannes, Laura Inés Nahabetián Brunet – Florianópolis: CONPEDI, 2024.

Inclui bibliografia
ISBN: 978-85-5505-986-5
Modo de acesso: www.conpedi.org.br em publicações
Tema: ESTADO DE DERECHO, INVESTIGACIÓN JURÍDICA E INNOVACIÓN

1. Direito – Estudo e ensino (Pós-graduação) – 2. Governo digital. 3. Novas tecnologias. XIII ENCONTRO INTERNACIONAL DO CONPEDI URUGUAI – MONTEVIDÉU (2: 2024 : Florianópolis, Brasil).

CDU: 34



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

XIII ENCONTRO INTERNACIONAL DO CONPEDI URUGUAI – MONTEVIDÉU

GOVERNO DIGITAL, DIREITO E NOVAS TECNOLOGIAS I

Apresentação

O XIII ENCONTRO INTERNACIONAL DO CONPEDI URUGUAI – MONTEVIDÉU, realizado na Universidad de La República Uruguay, entre os dias 18 a 20 de setembro de 2024, apresentou como temática central "Estado de Derecho, Investigación Jurídica e Innovación". Esta questão suscitou intensos debates desde o início e, no decorrer do evento, com a apresentação dos trabalhos previamente selecionados, fóruns e painéis que ocorreram na cidade de Montevidéu-Uruguai.

Os trabalhos contidos nesta publicação foram apresentados como artigos no Grupo de Trabalho "DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I", realizado no dia 20 de setembro de 2024, que passaram previamente por no mínimo dupla avaliação cega por pares. Encontram-se os resultados de pesquisas desenvolvidas em diversos Programas de Pós-Graduação em Direito, que retratam parcela relevante dos estudos que têm sido produzidos na temática central do Grupo de Trabalho.

As temáticas abordadas decorrem de intensas e numerosas discussões que acontecem pelo Brasil, com temas que reforçam a diversidade cultural brasileira e as preocupações que abrangem problemas relevantes e interessantes, a exemplo do direito digital, proteção da privacidade, crise da verdade, regulamentação de tecnologias, transformação digital e Inteligência artificial, bem como políticas públicas e tecnologia.

Espera-se, então, que o leitor possa vivenciar parcela destas discussões por meio da leitura dos textos. Agradecemos a todos os pesquisadores, colaboradores e pessoas envolvidas nos debates e organização do evento pela sua inestimável contribuição e desejamos uma proveitosa leitura!

Danielle Jacon Ayres Pinto - Universidade Federal de Santa Catarina

Yuri Nathan da Costa Lannes - Faculdade de Direito de Franca

Laura Inés Nahabetián Brunet - Universidad Mayor de la República Oriental del Uruguay

O DIREITO PENAL E A PROTEÇÃO DOS DIREITOS FUNDAMENTAIS NO AMBIENTE VIRTUAL: UMA ANÁLISE A PARTIR DA LEGISLAÇÃO BRASILEIRA.

CRIMINAL LAW AND THE PROTECTION OF FUNDAMENTAL RIGHTS IN THE VIRTUAL ENVIRONMENT: AN ANALYSIS FROM BRAZILIAN LEGISLATION.

Marília Freitas Lima

Resumo

O fim do século XX foi marcado pelo intenso desenvolvimento tecnológico que desencadeou na alteração da estrutura das sociedades capitalistas, acrescentando as interações pelas redes como um elemento basilar e integrativo. O que resultou na ampliação dos espaços, através do chamado ciberespaço, em que as pessoas interagem pessoalmente, e também, sócio-economicamente. Esta nova esfera é mais uma fronteira ao cometimento de delitos, porém, em uma perspectiva diferente do mundo real, o que exige novas formas de investigação e de agir. Este trabalho pretende analisar os principais desafios da aplicação da norma penal aos delitos cometidos no ambiente virtual, aprofundando nos estudos sobre autoria e territorialidade. As dificuldades de identificação do perfil dos usuários (e de conferência da real identificação) trazem desafios para as investigações criminais. Outro ponto, é a aplicação da norma jurídica, vez que o princípio da territorialidade é atrelado ao conceito clássico de território, rompido com a criação do ciberespaço. A fim de ampliar o debate, a presente pesquisa se utilizará do método bibliográfico-documental para compreender as principais políticas públicas e as modificações do direito brasileiro implementadas no combate ao cibercrime.

Palavras-chave: Direito penal, Ciberespaço, Metaverso, Crimes cibernéticos, Democracia digital

Abstract/Resumen/Résumé

The end of the 20th century was marked by intense technological development that led to changes in the structure of capitalist societies, adding interactions through networks as a basic and integrative element. This resulted in the expansion of spaces, through the so-called cyberspace, in which people interact personally, and also, socio-economically. This new sphere is yet another frontier for committing crimes, however, from a different perspective than the real world, which requires new forms of investigation and action. This work aims to analyze the main challenges of applying criminal law to crimes committed in the virtual environment, delving deeper into studies on authorship and territoriality. Difficulties in identifying user profiles (and checking real identification) bring challenges to criminal investigations. Another point is the application of the law, since the principle of territoriality is linked to the classic concept of territory, broken with the creation of cyberspace. In order

to broaden the debate, this research will use the bibliographic-documentary method to understand the main public policies and changes to Brazilian law implemented to combat cybercrime.

Keywords/Palabras-claves/Mots-clés: Criminal law, Cyberspace, Metaverse, Cybercrimes, Digital democracy

INTRODUÇÃO.

Ao longo do século XX, com o avanço da tecnologia e a criação de ambientes de trocas e relações através da internet, houve uma significativa alteração da vida humana. Intensificado no século XXI, com o vasto desenvolvimento do ciberespaço, as relações se tornaram mais complexas em todos os âmbitos, seja econômico, social ou cultural. Este contexto, que Castells (1999) chamou de sociedade em rede, apresenta uma interação determinante entre a sociedade e a tecnologia, pela qual "a tecnologia (ou sua falta) incorpora a capacidade de transformação das sociedades, bem como os usos que as sociedades, sempre em um processo conflituoso, decidem dar ao seu potencial tecnológico" (Castells, 1999).

O ciberespaço, para Pierre Lévy (1999), é um novo ambiente de comunicação, criado a partir da interconexão mundial dos computadores e a uma imensidão de informações abrigadas por ela, em que, para além da infraestrutura, se desenvolve uma cultura própria, a chamada cibercultura.

A sociedade digital influencia diretamente a vida cotidiana, as relações sociais, o governo, a economia e também na criação e disseminação de conhecimento (Lupton, 2015). Sendo assim, para além do ambiente real, torna-se mais uma possibilidade em que as pessoas criam, recriam, compartilham ideais e concepções de mundo, além de influenciar e serem influenciadas em suas próprias realidades. Não há, neste sentido, possibilidade de dissociar o impacto das tecnologias digitais e as implicações de seu uso do aspecto político, vez que a serventia dessas tecnologias está atrelada à orientação política consolidada/dominante.

As normas, e aqui especialmente as criminais, passam a ser demandadas para ampliar o controle sobre as ações desviantes que ocorrem naquele ambiente. Por ser um mundo organizado e gerido por grandes corporações de tecnologia, o que se pergunta com esta pesquisa é se é possível estender as reprimendas e sanções estatais às infrações que lá ocorrem.

A fim de responder ao questionamento acima, serão analisadas as legislações nacionais sobre o tema e as políticas públicas de combate aos crimes cibernéticos. Além de compreender se é possível ampliar essa normatização para aquele espaço. Para tanto, se utilizará de método hipotético-dedutivo, através de bibliografia nacional e internacional sobre a temática.

Metodologicamente, este trabalho se divide em quatro tópicos: o primeiro irá abordar o ciberespaço e a ampliação do uso da tecnologia; o segundo tratará das políticas públicas nacionais para o combate aos cibercrimes; o terceiro analisará a legislação sancionadora

nacional sobre os crimes cometidos na internet; e, por fim, o último tópico abordará o metaverso com mais uma fronteira para o cometimento de novos delitos.

1 Criação do ciberespaço e o uso da tecnologia.

Um aspecto dos tempos atuais é a indissociação entre o humano e a tecnologia. A grande dependência da experiência humana com as interações através das redes sociais faz com que o mundo real e o mundo virtual se tornem interligados. E este lugar é denominado de ciberespaço. Nas palavras de Manuel Castells (1999), "a revolução da tecnologia da informação foi essencial para a implementação de um importante processo de restruturação do sistema capitalista a partir da década de 80". Com as novas tecnologias da informação integra o mundo através de redes. Nesse contexto, ressalta que o espaço público e as interações entre governo, empresas e organizações é mediado pelas tecnologias digitais. Em que as redes estruturam as sociedades contemporâneas e as relações de poder.

> *Digital data objects structure our concepts of identity, embodiment, relation ships, our choices and preferences and even our access to services or spaces. There are many material aspects to digital data. They are the product of complex decisions, creative ideas, the solving and manage ment of technical problems and marketing efforts on the part of those workers who are involved in producing the materials that create, manage and store these data. They are also the product of the labour of the prosumers who create the data*. (Lupton, 2023)

As modificações trazidas pela incorporação da tecnologia à estrutura social faz uma alteração nas identidades, preferências, inclusive nas escolhas pessoais. Na chamada era digital, há o esfacelamento dos "vínculos éticos de alteridade" (Nunes, 2018), das relações em comunidade, em um contexto de hiperindividualismo. Assim sendo, a criminologia e o direito penal precisaram construir, também, novos paradigmas. Se de um lado há a modificação do Estado Social para o Estado Penal (Wacquant, 2015) através da culpabilização do indivíduo e o aumento do controle e vigilância, por outro surge a demanda de regulamentação desse novo espaço de interação e, consequentemente, novos tipos penais são criados.

A dimensão globalizada faz a captação dos dados pessoais e, através deles, formam um corpo eletrônico. Essa acumulação de informações cria "nossos hábitos de consumo, do nosso círculo de amizades, de nossas simpatias políticas, de nossas tendências ideológicas, de nossos gostos" (Fachinni Neto, 2023).

Se a tecnologia surgiu de maneira contundente no fim do século XX, é no século XXI que, através de um aprofundamento na revolução digital, com o entrelaçamento entre o físico, o digital e o biológico. Isso é demonstrado através do uso do metaverso e da inteligência artificial.

> Em visão concorrente, Klaus Schwab, diretor-presidente do Fórum Econômico Mundial, publicou, em 2016, "A Quarta Revolução Industrial"2, que é o nome que ele dá à época em que passamos a viver nas duas últimas décadas, como um aprofundamento da revolução digital. Ela é caracterizada "por uma internet mais ubíqua e móvel, por sensores menores e mais poderosos que se tornaram mais baratos, e pela inteligência artificial e aprendizagem automática (ou aprendizado de máquina)." A razão do seu caráter disruptivo em relação à terceira revolução industrial (relacionada ao advento da computação e da internet) é que essas novas tecnologias estão se tornando mais sofisticadas e integradas, envolvendo a fusão e interação de domínios físicos, digitais e biológicos, envolvendo aspectos tão distintos quanto sequenciamento genético, nanotecnologia, energias renováveis e computação quântica. (Fachinni Neto, 2023).

Esse ambiente de novas tecnologias é entendido como ciberespaço ou rede, que, para Pierre Lévy (1999) "é o novo meio de comunicação que surge da interconexão mundial dos computadores". Essa terminologia se refere tanto à infraestrutura que estabelece a comunicação digital, como também a todas as informações enviadas e armazenadas por ela.

Já a cibercultura, que se desenvolve dentro desse espaço interativo, se apresenta de duas formas (Lévy, 1999): diretamente, pela digitalização das informações; e, indiretamente, pelo desenvolvimento de redes digitais que promovem interações entre os usuários. Assim, a comunicação ocorrida no mundo real, também passa a ocorrer no virtual. E todas as demais interações também - comércio, trocas, negócios, relacionamentos e delitos.

2 O aumento do uso da internet e o combate aos cibercrimes: políticas públicas nacionais para o combate a essa modalidade criminal.

De acordo com a pesquisa nacional TIC Domicílios, aplicada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação - Cetic.Br (2023), o Brasil, no ano de 2022, chegou ao percentual de 80% dos seus domicílios com acesso à internet. No ano de 2015, eram apenas 51% de domicílios conectados à rede. Quanto à cobertura, 86% estão na área urbana e 74% na área rural. Quanto aos aparelhos utilizados, na área urbana usam: 94% televisão e 95% telefone celular; na área rural: 91% televisão e 92% celular.

Durante a pandemia no Covid-19, um dos impactos relevantes foi o aumento do uso da internet, a partir da necessidade de adaptação das atividades de trabalho e de educação. À época, a TIC Domicílios 2020, uma edição com metodologia adaptada, identificou um importante aumento no acesso às redes. Em comparação ao período de 2019, houve um aumento de 12% nos domicílios com acesso à rede e 7% no número de usuários (Cetic, 2021).

> A pesquisa reiterou o aumento na realização de atividades *on-line* durante a pandemia, que havia sido identificada anteriormente pelo **Painel TIC COVID-19**. No entanto, a pesquisa mostrou que desigualdades no aproveitamento das oportunidades *on-line* ainda persistem. Usuários da Classe C, por exemplo, realizaram mais cursos a distância e estudaram mais por conta própria em 2020 em relação a 2019, mas ainda em proporções inferiores aos usuários da classe A.
> Segundo o levantamento, mais usuários procuraram (42%), ou realizaram (37%) serviços públicos *on-line* em 2020. Essas atividades concentraram-se mais entre moradores de áreas urbanas, com mais escolaridade e das classes A e B. Houve também crescimento da realização de transações financeiras no ambiente digital (43%, contra 33% em 2019), com aumento mais expressivo entre aqueles das classes C e DE. (Cetic, 2021)

É importante ressaltar que no momento da pandemia houve uma readaptação das atividades presenciais para o mundo virtual. Onde, muito rapidamente, as pessoas alteraram suas rotinas e precisaram se adaptar a uma nova realidade exigida pelo isolamento social necessário. Com isso, há uma expansão no uso do ambiente digital para o trabalho e também para os estudos, inclusive pelas parcelas mais vulneráveis da população. Apesar dos avanços, as pesquisas TIC Domicílio ainda mostram, por seus indicadores, a persistência em uma desigualdade de acesso, sendo maior nas classes mais altas e entre os jovens e escolarizados.

O uso da internet permite o acesso a um novo ambiente relacional, onde contratos são firmados, serviços são executados e informações são compartilhadas. Neste sentido, também se torna um ambiente em que crimes, assim como no mundo real, também são cometidos.

Sobre isso, em 2022, a Fortinet, uma empresa especializada em serviços de cibersegurança, realizou uma pesquisa que indicou que o Brasil ocupou o segundo lugar em números de ataques cibernéticos dentre os países da América Latina e Caribe. No ano de 2021, foram 88,5 bilhões de tentativas de ataques cibernéticos, ficando atrás apenas do México, que registrou 156 bilhões de ataques.

Dentre esses ataques, a utilização de envio de *phishing* por e-mail foi a mais utilizada, além da distribuição de *malware* por publicidade enganosa e o uso de sites

maliciosos. Ocorre que a finalidade dos criminosos é infectar os dispositivos das vítimas e controlá-los, cometendo, assim, crimes cibernéticos. No tempo desta pesquisa, em 2021, observou-se o uso de informações sobre a covid-19 e a transmissão da variante ômicrom como pano de fundo para intensificarem os roubos de informações de usuários (Fortinet, 2022).

Outra pesquisa que apresenta subsídios entre o uso da internet e o contexto da pandemia é o Anuário Brasileiro de Segurança Pública que, em sua edição de 2023, apresenta um aumento nos crimes de estelionato (art. 171, do Código Penal) ocorridos via *internet*, apresentando 200.322 registros de ocorrências, representando um aumento de 65,2% em relação ao ano de 2021. Diferentemente dos crimes de roubo e furtos que apresentaram queda durante aquele período, o estelionato por redes sociais e aplicativos de mensagens cresceram em vários países do mundo, inclusive, no Brasil.

Ressalta-se que é um fenômeno que não se restringe à análise de segurança ou da necessidade de letramento digital, vez que "os estudos indicam é que os criminosos têm explorado fatores situacionais ao identificar vítimas mais vulneráveis, diversificado os métodos de ataque e empregado técnicas de engenharia social (induzir usuários a enviar dados confidenciais)" (Fórum Brasileiro de Segurança Pública, 2023).

A pandemia foi um fator que acelerou a migração das relações do mundo real para o digital, o que demandou uma adaptação pelos usuários e também por parte das forças de segurança. O próprio estudo do Anuário Brasileiro de Segurança Pública (2023) apresenta três fatores desafiadores para as investigações deste tipo de crime: o crescimento acelerado de fraudes e estelionatos eletrônicos; a diferença entre os limitados recursos investigativos disponíveis e a quantidade de crimes registrados, especialmente, quanto à disponibilidade de recursos humanos, financeiros e técnicos; e, por fim, a formação insuficiente dos policiais que atendem as ocorrências, vez que exigiria o acesso a cursos de alta especialização, além de rígida rotina de atualização, vez que no ambiente tecnológico as mudanças acontecem de maneira muito rápida.

A conclusão a que se chega é que "O investimento nas polícias judiciárias, em especial as polícias civis estaduais, é fator estratégico que fará toda a diferença no enfrentamento dos novos arranjos e dinâmicas criminais" (Fórum Brasileiro de Segurança Pública, 2023).

A fim de melhorar a estrutura policial de investigação, no ano de 2022, foi criada, no âmbito da Polícia Federal, a Unidade Especial de Investigação de Crimes Cibernéticos (UEICC). É uma das criações que surgiram da parceria público-privada entre o Ministério da

Justiça e Segurança Pública juntamente com a Federação Brasileira de Bancos, com o objetivo de intercambiar informações para prevenção e resolução de crimes cibernéticos, especialmente, as fraudes bancárias que, entre os anos de 2020-2022, representaram somaram R$ 8 bilhões, dentre os quais, os criminosos obtiveram êxito em R$2 bilhões (MJSP, 2022).

Além disso, no ano de 2023, através do Decreto nº 11.856, foi instituída a Política Nacional de Cibersegurança (PNCiber) e o Comitê Nacional de Cibersegurança (CNCiber). Tem como finalidade orientar a segurança cibernética no país e apresenta como princípios:

> Art. 2º São princípios da PNCiber:
> I - a soberania nacional e a priorização dos interesses nacionais;
> II - a garantia dos direitos fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação;
> III - a prevenção de incidentes e de ataques cibernéticos, em particular aqueles dirigidos a infraestruturas críticas nacionais e a serviços essenciais prestados à sociedade;
> IV - a resiliência das organizações públicas e privadas a incidentes e ataques cibernéticos;
> V - a educação e o desenvolvimento tecnológico em segurança cibernética;
> VI - a cooperação entre órgãos e entidades, públicas e privadas, em matéria de segurança cibernética; e
> VII - a cooperação técnica internacional na área de segurança cibernética.

No seu texto também estabelece o Comitê Nacional de Cibersegurança - CNCiber, instalado na Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo, a fim de acompanhar a implementação da referida Política Nacional. Atualmente, sua composição se dá através de 16 membros permanentes, compostos por representantes governamentais, bem como 09 representantes da sociedade civil (GSI, 2024).

Esta legislação surge a partir das articulações ocorridas, inicialmente, pela aprovação da Estratégia Nacional de Segurança Cibernética (E-Ciber), criada pelo Decreto nº 10.222/2010, com validade para o quadriênio 2020-2023. Fora estabelecida pelo trabalho de 3 subgrupos de trabalho que possuíam as seguintes finalidades: governança cibernética, dimensão normativa, pesquisa, desenvolvimento e inovação, educação, dimensão internacional e parcerias estratégias; confiança digital e prevenção e mitigação de ameaças cibernéticas; e, proteção estratégica - proteção do Governo e proteção às infraestruturas (BRASIL, 2020).

Posteriormente, foi desenvolvido o projeto da Política Nacional Cibersegurança (PNCiber) e Sistema Nacional de Cibersegurança (SNCiber), no ano de 2023. O projeto justifica a opção pelo uso do modelo de agência reguladora, como uma possibilidade

consolidada no "'institucionalismo histórico' da nossa sociedade" e porque a "autonomia confere considerável estabilidade às instituições quanto a eventuais instabilidades políticas ou econômicas". Além disso, o projeto aponta que "outros modelos recentemente testados se mostraram frágeis nos quesitos acima mencionados, e foram (ou vêm sendo) gradualmente adaptados para se aproximarem do modelo de agências regulatórias" (BRASIL, 2023).

Outro dado importante levantado na exposição de motivos é a ampla utilização, pela Administração Pública, do meio digital. Citando a Lista de Alto Risco na Administração Pública, elaborada pelo Tribunal de Contas da União (TCU), em 2021, 73,1% dos serviços públicos prestados pelo governo federal eram totalmente digitais. Considerando os parcialmente digitais, esse número chega ao percentual de 86,7% (BRASIL, 2023).

2.1 Cibercrimes e a previsão no Código Penal Brasileiro.

No cenário brasileiro, foram demandados especialmente, aqueles que se referem a criminalização de condutas contra a liberdade individual e contra a dignidade sexual. A primeira legislação criada foi a Lei nº 12.737/2012, que criminaliza a invasão a dispositivo informático (art. 154-A). Esta lei foi apelidada de Lei Carolina Dieckmann, em virtude do caso que tomou proporções midiáticas naquele tempo.

A atriz teve o seu computador invadido por um *hacker*, que obteve ilicitamente 36 fotos íntimas, objeto de posterior extorsão. Após dois anos após a divulgação das imagens da atriz, a legislação foi aprovada (Araújo, 2023). Além do crime acima, essa legislação alterou o art. 266 - Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública - e o art. 298 - Falsificação de cartão (Brasil, 2012).

Posteriormente, outras duas importantes legislações foram criadas: a Lei 13.772/2018 e a Lei 13.772/2018. A primeira alterou a Lei Maria da Penha, acrescentando o conceito de violência psicológica, que passa a ser entendida como:

> qualquer conduta que lhe cause dano emocional e diminuição da autoestima ou que lhe prejudique e perturbe o pleno desenvolvimento ou que vise degradar ou controlar suas ações, comportamentos, crenças e decisões, mediante ameaça, constrangimento, humilhação, manipulação, isolamento, vigilância constante, perseguição contumaz, insulto, chantagem, violação de sua intimidade, ridicularização, exploração e limitação do direito de ir e vir ou qualquer outro meio que lhe cause prejuízo à saúde psicológica e à autodeterminação (Brasil, 2018a)

Além disso, cria o crime de registro não autorizado da intimidade sexual (art. 216-B), que tipifica a conduta daquele que "produzir, fotografar, filmar ou registrar, por qualquer meio, conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado sem autorização dos participantes". Além, daquele que "realiza montagem em fotografia, vídeo, áudio ou qualquer outro registro com o fim de incluir pessoa em cena de nudez ou ato sexual ou libidinoso de caráter íntimo" (Brasil, 2018a).

Logo após, é promulgada a Lei 13.718/2018 que "tipifica os crimes de importunação sexual e de divulgação de cena de estupro, torna pública incondicionada a natureza da ação penal dos crimes contra a liberdade sexual e dos crimes sexuais contra vulnerável, estabelece causas de aumento de pena para esses crimes e define como causas de aumento de pena o estupro coletivo e o estupro corretivo" (Brasil, 2018b). Esta legislação amplia a proteção aos crimes sexuais e insere, especificamente, no art. 218-C, § 1º, um aumento de pena para a figura da pornografia de vingança.

Em seguida, houve a aprovação da Lei 14.132, em março de 2021, que acrescentou o art. 147-A ao Código Penal, para prever o crime de perseguição e revogou o art. 65 da Lei das Contravenções Penais. A partir desta legislação, se considera crime "perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade" (Brasil, 2021).

Ainda, recentemente, a aprovação de legislação específica para a proteção contra a intimidação sistemática por meios virtuais - crime de cyberbullying, adicionando o art. 146-A - Lei nº 14.811/2024.

3 Crimes cometidos no Metaverso

Um novo fenômeno que surge com o desenvolvimento tecnológico, principalmente, com a ampliação do uso da inteligência artificial é a criação e uso do metaverso. Metaverso é a combinação do prefixo "meta" (além) e o sufixo "verso" (universo). Trata-se de um mundo para além do real, criado através da tecnologia digital. Neste ambiente, as pessoas passam por experiências de grande realismo e profunda imersão (Wu *et al*, 2023).

O construção do metaverso, enquanto mundo virtual interativo, pode ser classificada em duas etapas: o Web2, que é centralizado nas grandes corporações de tecnologia, em que há o controle e a propriedade ligados a elas - chamado de "*closed corporate metaverse*"; e, o

Web3, que é descentralizado e a propriedade é dos membros da comunidade - denominado de "*open crypto metaverse*" (Wu *et al*, 2023).

Com o desenvolvimento e maior utilização do metaverso Web3, os crimes começaram a se tornar mais complexos e a se diversificarem. A exemplo da ampliação do cometimento de crimes financeiros que envolvem a transferência ilegal de valores, como fraudes e lavagem de dinheiro.

> *Along with the recent development of Web3, financial crimes have been given a more diverse and complex meaning in the metaverse ecology. Based on the employment of blockchain in metaverse, many fraudsters have found new opportunities for illicit profits, including money laundering, identity theft, and scams.* (Wu *et al*, 2023)

A Web3 é formada por uma rede controlada pelos próprios usuários e pelos criadores dos conteúdos. O benefício que pregam é melhorar a capacidade da gestão dos recursos, bem como uma maior segurança dos dados dos usuários e a responsabilização individual pelas interações *online*. Neste ambiente, os usuários criam avatares para vivenciar diversas experiências de imersão social, além de realizarem trocas financeiras através do sistema *blockchain*[1].

Claro que, ao mesmo tempo que surge uma tecnologia inovadora, também se apresentam os riscos trazidos com ela. E o maior desafio jurídico é a ampliação dos conceitos de tempo e de espaço. Antes mesmo de serem construídas soluções viáveis e legislações específicas sobre os crimes que ocorrem naquele ambiente virtual, é certo perceber que já estamos imersos nele. Ou seja, ao mesmo tempo que o utiliza, tenta-se compreendê-lo e regulamentá-lo.

No ano de 2023, a Interpol organizou uma lista com os principais metacrimes reportados a ela, que incluiam: fraudes em NFT, ataques cyberfísico, roubo de identidades virtuais, roubo de propriedades 3D e ativos virtuais, corrupção de menores, perseguição e e assédio sexual virtual.

> *With its increasing use and the number of participants, there is a need to define what constitutes crimes and harms in the Metaverse. Defining crimes and criminalizing harmful actions are essential for ensuring the safety and security of the Metaverse, as effective policing and law enforcement responses depend on clear legislation*. (Interpol, 2024)

[1] *"in Web3, application data is no longer stored in a private database but in a blockchain that can be written or read by anyone. Blockchain returns digital sovereignty to the users through a decentralized manner. There exist three main types of blockchain: public, private and consortium [5], and one of the typical applications of the public blockchain is the Bitcoin."* (Wu *et al*, 2023)

A ampliação do número de usos de participantes do metaverso possibilita um incremento no número e tipos de crimes cometidos, o que também exige uma resposta jurídica a isso. Tão faz parte de nossa realidade, que é possível citar exemplos de como é um instrumento presente na vida e nas relações pessoais e profissionais. No ano de 2022, o Tribunal de Justiça do Estado de Goiás, na Comarca de Anápolis, foi, de forma inédita, adotado o uso de ambiente virtual que simula um espaço compartilhado entre advogados e a magistrada. Por não haver regulamentação formal para este uso, atualmente, é utilizado para situações administrativas e reuniões (Santana, 2022).

Já em setembro daquele mesmo ano, a Justiça Federal na Paraíba realizou a primeira audiência real no metaverso. Foi uma audiência de conciliação em que as partes envolvidas - autor e réu - estavam presentes através de seus avatares, customizados em 3D e, como resultado, firmaram um acordo judicial para finalização do processo em curso (Cnj, 2022).

O uso imersivo da tecnologia trouxe inúmeras outras possibilidades para trocas financeiras virtuais, compras, estudos, lazer e negócios. O que possibilitou uma maior disponibilidade de dados pessoais para as empresas que fazem a gestão desses ambientes e um controle dessas informações. Ainda que muitas possuam políticas internas de organização e garantia de sigilo de muitos desses dados, ainda há um grande desafio em garantir ao usuário uma plena segurança nas suas conexões no ambiente virtual.

Quanto à aplicação da norma jurídica, dois pontos de fragilidade se mostram: a autoria e a jurisdição a ser aplicada. Em algumas atividades criminais cometidas no metaverso, alguns avatares conseguem fraudar a sua própria identidade. Eles podem, por vezes, serem utilizados como intermediários entre as pessoas e atividades ilícitas, criando falsas identidades ou atraindo pessoas a engajarem tais feitos (Interpol, 2024).

A criação de perfis para avatares irá variar em cada plataforma a ser utilizada: algumas exigem a apresentação de uma carteira criptografa, enquanto outras apenas exigem um endereço válido de e-mail e um documento de identificação. Essa ausência de padronização é um dos grandes desafios não apenas para as plataformas, mas também para a aplicação das legislações.

Sendo assim, existem dois tipos de informações a serem tratadas pelas plataformas e pelas autoridades: as informações de identidade compartilhadas com as plataformas (*user-to-service*) e aquelas usadas entre os usuários (*user-to-user*), vez que podem optar por utilizar diferentes apresentações no mudo virtual. Podendo os avatares serem entendidos

como "*a digital entity that can be used as a (visual) representation of the user inside the virtual environments*" (Interpol, 2024).

Sendo uma representação e podendo realizar ações naquele ambiente, é necessário estabelecer a natureza jurídica dos avatares e isso é decisivo para delimitar as extensões de suas ações. É possível classificá-lo, atualmente, em quatro perspectivas: a) extensão do ser humano; b) representação simbólica do ser humano; c) propriedade do ser humano; d) persona legalmente anônima (Interpol, 2024).

A depender da forma que se entende o avatar dentro do sistema legal, haverá uma maneira de se responsabilizar quanto aos danos quanto às atividades criminosas. Urge, portanto, a necessidade do desenvolvimento de uma compreensão padrão sobre o que se entende por avatar, o que reduziria as divergências e lacunas entre os diferentes sistemas jurídicos, especialmente, por ser um tema de consequência transacional.

Outro problema que subsiste é a escolha de qual jurisdição a ser aplicada vez que, tradicionalmente, se pressupõe a existência de um território. Para a aplicação da jurisdição de um país sobre o outro, é preciso estabelecer algum mecanismo de cooperação internacional.

> E em se tratando de internet, o conceito tradicional de soberania, que preceitua que o Estado deverá exercer sua autoridade pela e governo próprio, dentro do território nacional e em suas relações com outros Estados, precisa ser reavaliado. Isso porque uma das características principais da grande rede é o fato de o indivíduo restaurar múltiplas relações por meio eletrônico sem que o Estado possa efetivamente controlá-lo. (Pompilio; Rechsteiner; 2022)

O esfacelamento das fronteiras do Estado Moderno e o questionamento das suas fronteiras é uma das características da pós-modernidade, através da expansão da globalização, seja em aspectos econômicos, mas também sociais. As normas comerciais e civis já avançaram bastante nas regulamentações próprias, mas as normas penais ainda possuem dificuldade dada as suas características principiológicas. E isso também se estende ao surgimento de uma nova realidade, que é o metaverso.

A soberania é elemento fundamental do Estado Moderno, sendo uma entidade política que estabelece as regras impostas dentro de seu território. No entanto, a transformação espacial trazida pela internet "altera o exercício do poder sobre fatos nacionais, na medida em que estes agora se alastram mundialmente" (Pompilio; Rechsteiner;2022)

Até o presente momento, os países conseguem investigar e processar crimes que, embora cometidos naquele espaço, possuem reflexo no mundo real, como as fraudes financeiras e a lavagem de dinheiro. Porém, outros crimes que afetam direitos da

personalidade, ainda são de difíceis respostas jurídicas. Neste ano, de forma inédita, a polícia britânica abriu investigação sobre um crime de estupro virtual praticado em um ambiente metaverso, no qual uma jovem de 16 anos, que participava de um jogo de realidade virtual, teve seu avatar atacado por um grupo de avatares de homens adultos. Apesar da ausência do dano físico, pela realidade virtual proporcionar sensações e ser hiper realista, foram gerados danos psicológicos e emocionais na vítima (Alves, 2024).

Pela ausência de regulamentação específica e ainda os questionamentos jurídicos existentes, é urgente a ampliação do debate para a criação de mecanismos efetivos de cuidado e proteção aos usuários, bem como de instrumentos sancionatórios eficazes.

CONSIDERAÇÕES FINAIS.

Não há como, na atualidade, dissociar as atividades humanas do uso das tecnologias digitais, sendo suas implicações percebidas em todos os aspectos da vida. As normas penais, neste sentido, aparecem em dois aspectos: tanto como controle e hipervigilância, quanto como proteção aos direitos fundamentais do cidadão. Uma contradição de um instrumento que ainda é necessário dentro da estrutura social.

O Brasil avançou no debate e na proteção aos crimes cibernéticos, especialmente nos últimos dez anos. Foram construídas políticas integrativas entre entes públicos e privados que possibilitaram a criação de uma rede de proteção. Além disso, houve uma atenção legislativa aos delitos contra a dignidade sexual, bem como à liberdade individual.

Porém, o espaço que ainda entra em uma lacuna legislativa é o metaverso. Por não ter legislação específica e por ainda haver grandes discussões quanto à natureza dos avatares que o compõem, apresenta uma grande fragilidade quando se torna palco de crimes. Este trabalho teve a pretensão de apresentar o debate sobre a aplicação da lei penal e os desafios que ainda se apresentam à definição clássica de autoria e território.

Os debates estão postos, mas exige um esforço político e legislativo dos países, vez que as consequências daqueles delitos são transnacionais. Algumas iniciativas importantes já estão implementadas, como a instalação da Interpol no metaverso, bem como as operações da Polícia Federal, no caso brasileiro. No entanto, entende-se que no campo teórico o debate ainda precisa avançar para trazer as definições necessárias para uma melhor efetividade dos mecanismos de proteção que atualmente existem.

REFERÊNCIAS.

ALVES, Ana Margarida. **Polícia britânica investiga violação virtual em grupo de jovem de 16 anos.** Publicado em 05 jan 2024. Disponível em: https://www.publico.pt/2024/01/05/p3/noticia/policia-britanica-investiga-violacao-virtual-grupo-jovem-16-anos-2075705. Acesso em 05 jun 2024.

ARAÚJO, Janaína. **Dez anos de vigência da Lei Carolina Dieckmann**: a primeira a punir crimes cibernéticos. Publicado em 29/03/2023. Disponível em: https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmann-a-primeira-a-punir-crimes-ciberneticos. Acesso em 05 jun 2024.

BRASIL. **Decreto nº 10.222, de 05 de fevereiro de 2020** - Aprova a Estratégia Nacional de Segurança Cibernética. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em 01 jun 2024.

BRASIL. **Decreto nº 11.856, de 26 de dezembro de 2023** - Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm. Acesso em 02 jun 2024.

BRASIL. **Lei 12.737, de 30 de novembro de 2012** - Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 05 jun 2024.

BRASIL. **Lei nº 13.772, de 19 de dezembro de 2018** - Altera a Lei nº 11.340, de 7 de agosto de 2006 (Lei Maria da Penha), e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) [...]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13772.htm. Acesso em 05 jun 2024.

BRASIL, **Lei nº 13.718, de 24 de setembro de 2018** - Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar os crimes de importunação sexual e de divulgação de cena de estupro [...]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13718.htm. Acesso em 05 jun 2024.

BRASIL. **PNCiber** – Apresentação do Projeto (2023). Disponível em: https://www.gov.br/gsi/pt-br/ssic/audiencia-publica/PNCiberAudienciaPublicaProjetoBase.pdf. Acesso em 02 jun 2024.

CETIC. **Cresce o uso de Internet durante a pandemia e número de usuários no Brasil chega a 152 milhões, é o que aponta pesquisa do Cetic.br**. Publicado em 18 ago 2021. Disponível em: https://cetic.br/pt/noticia/cresce-o-uso-de-internet-durante-a-pandemia-e-numero-de-usuarios-no-brasil-chega-a-152-milhoes-e-o-que-aponta-pesquisa-do-cetic-br/. Acesso em 01 jun 2024.

CASTELLS, Manuel. **A sociedade em rede**. 6ª ed. São Paulo: Paz e Terra, 1999.

CETIC. **TIC Domicílios 2023**. Disponível em: https://cetic.br/pt/tics/domicilios/2023/domicilios/A/. Acesso em 01 jun 2024.

CNJ. **Justiça Federal na Paraíba realiza primeira audiência real do Brasil no metaverso.** Publicado em 15 set de 2022. Disponível em: https://www.cnj.jus.br/justica-federal-na-paraiba-realiza-primeira-audiencia-real-do-brasil-no-metaverso/. Acesso em 06 jun 2024.

FACCHINI NETO, Eugênio. **Mundo digital, algoritmos e perfilização**: detectando os perigos de um nem sempre admirável mundo novo. *In*. TRINDADE, André Karam; BUSSINGUER, Elda Coelho de Azevedo; SARLET, Ingo Wolfgang. **Estado, Regulação e Transformação Digital**: o futuro das democracias - hipervigilância, fake news e outras ameaças. São Paulo: Tirant lo Blanch, 2023.

FORTINET. **Brasil sofreu mais de 88,5 bilhões de tentativas de ataques cibernéticos em 2021**. Publicado em 08 fev 2022. Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-relatorio-ciberataques-brasil-2021. Acesso em 01 jun 2024.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **17º Anuário Brasileiro de Segurança Pública**. São Paulo: Fórum Brasileiro de Segurança Pública, 2023. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2023/07/anuario-2023.pdf. Acesso em: 01 jun 2024.

GSI. Gabinete de Segurança Institucional. **Comitê Nacional de Cibersegurança**. Disponível em: https://www.gov.br/gsi/pt-br/colegiados-do-gsi/comite-nacional-de-ciberseguranca-cnciber. Acesso em 01 jun 2024.

INTERPOL. **Metaverse**: a law enforcement perspective: use cases, crime, forensics, investigation, and governance. Publicado janeiro/2024. Editora White Paper. Disponível em: https://www.interpol.int/content/download/20828/file/Metaverse%20-%20a%20law%20enforcement%20perspective.pdf

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

LUPTON, Deborah. **Digital Sociology**. 1ª ed. Nova Iorque: Editora Routledge, 2015.

MJSP. Ministério da Justiça e Segurança Pública. **Polícia Federal cria Unidade Especial para intensificar a repressão a crimes cibernéticos**. Publicado em 28/06/2022. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/policia-federal-cria-unidade-especial-para-intensificar-a-repressao-a-crimes-ciberneticos. Acesso em 01 jun 2024.

POMPILIO, Isabela Braga; RECHSTEIMER, Sandra Alette Maia. **A transformação espacial do metaverso e os limites da jurisdição**. *In*. SEREC, Fernando Eduardo (coord). Metaverso: aspectos jurídicos. São Paulo: Almedina, 2022.

SANTANA, Vitor. **Juíza usa metaverso em reuniões e atendimentos a advogados em Anápolis**. Publicado em 21/09/2022. Disponível em: https://g1.globo.com/go/goias/noticia/2022/09/21/juiza-usa-metaverso-em-reunioes-e-atendimentos-a-advogados-em-anapolis.ghtml. Acesso em 06 jun 2024.

WU, Jiajing; *et al*. **Financial Crimes in Web3-Empowered Metaverse**: Taxonomy, Countermeasures, and Opportunities. IEEE Open Journal of the Computer Society. Publicado em 16 fev 2023. Disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10045768. Acesso em 06 jun 2024.