UNIVERSIDADE DE BRASÍLIA

INSTITUTO DE RELAÇÕES INTERNACIONAIS

NOELSON ARAÚJO BRAGA

CIBERSEGURANÇA E O DIREITO À PRIVACIDADE:

Um Estudo sobre a construção cibernética no Brasil e União Europeia sob a ótica realista

BRASÍLIA

2021

UNIVERSIDADE DE BRASÍLIA
INSTITUTO DE RELAÇÕES INTERNACIONAIS

Noelson Araújo Braga

CIBERSEGURANÇA E O DIREITO À PRIVACIDADE:

Um Estudo sobre a construção cibernética no Brasil e União Europeia na ótica realista

Trabalho de Conclusão de Curso apresentado à Universidade de Brasília (UnB) como requisito optativo para a obtenção do título de Bacharel em Relações Internacionais.

Orientador(a): Prof. Dr. Alcides Costa Vaz

Banca Examinadora:

Prof. Dr. Alcides Costa Vaz
IREL - UnB

Prof. Dr. Juliano Cortinhas da Silva
IREL-UnB

Profª. Drª. Norma Breda dos Santos
IREL UnB

BRASÍLIA
2021

RESUMO:

A cibersegurança é um desafio global que exige cooperação internacional e engajamento dos países na construção de aparato de defesa eficaz no combate de ciberameaças. Apesar da gama de ameaças e objetivos para alcançar um ciberespaço seguro, países como o Brasil têm utilizado de política nacional, enquanto a União Europeia adotou a política regional. Isso levanta questões acerca da importância do processo de evolução dos meios cibernéticos para compreender como os países passarão a lidar com as ciberameaças no futuro e como este processo afetará a proteção de dados e o direito à privacidade. O presente estudo tem por objetivo avaliar a construção da legislação sobre temas cibernéticos no Brasil, buscando como parâmetro o Regulamento Geral sobre a Proteção de Dados da União Europeia (RGPD) para embasar as configurações da atual Lei Geral de Proteção de Dados (LGPD) e os demais dispositivos que tratam do tema. Tem-se por objetivo compreender a progressão dos países e empresas nacionais e internacionais no combate às ameaças cibernéticas, e a dinâmica pela busca na cooperação e ciberdiplomacia sob uma ótica da teoria realista. Conclui-se que o processo que deu origem à LGPD foi essencial para a união de esforços multissetoriais no Brasil, mas que se limitaram ao campo doméstico, enquanto na União Europeia há resultados satisfatórios na projeção da cibersegurança como ferramenta de defesa e de desenvolvimento, mesmo que de forma lenta, e visando os interesses nacionais sobre as decisões coletivas.

Palavras-chave: Proteção de dados; cibersegurança; Lei Geral de Proteção de Dados - LGPD; Regulamento Geral sobre a Proteção de Dados - RGPD; direito à privacidade; realismo

ABSTRACT:

Cybersecurity is a global challenge that requires international cooperation and the engagement of countries in building an effective defense apparatus to combat cyber threats. Despite the range of threats and objectives to achieve a safe cyberspace, countries like Brazil have used national policy, while the European Union adopted regional policy. This raises questions about the importance of the evolving cybermedia process in understanding how countries will come to grips with cyber threats in the future and how this process will affect data protection and the right to privacy. This study aims to evaluate the construction of legislation on cyber issues in Brazil, seeking as a parameter the General Regulation on Data Protection of the European Union (RGPD) to support the configurations of the current General Data Protection Law (LGPD) and the other devices that deal with the topic. The objective is to understand the progression of national and international countries and companies in the fight against cyber threats, and the dynamics for the search for cooperation and cyberdiplomacy under the perspective of realist theory. It is concluded that the process that gave rise to the LGPD was essential for the union of multisectoral efforts in Brazil, but that they were limited to the domestic field, while in the European Union there are satisfactory results in the projection of cybersecurity as a defense and development tool, even that slowly, and targeting national interests over collective decisions.

Keywords: Data protection; cybersecurity; General Data Protection Law - LGPD; General Regulation on Data Protection - RGPD; right to privacy; Realism

RESUMEN:

La ciberseguridad es un desafío global que requiere cooperación y el compromiso de los países en la construcción de un aparato de defensa eficaz en la lucha contra las ciberamenazas. A pesar de la variedad de amenazas y objetivos para lograr un ciberespacio seguro, países como Brasil han utilizado la política nacional, mientras que la Unión Europea adoptó la política regional. Esto plantea preguntas sobre la importancia del proceso de cibermedios en evolución para comprender cómo los países enfrentarán las amenazas cibernéticas en el futuro y cómo este proceso afectará la protección de datos y el derecho a la privacidad. Este estudio tiene como objetivo evaluar la construcción de legislación en materia cibernética en Brasil, buscando como parámetro el Reglamento General de Protección de Datos de la Unión Europea (RGPD) para sustentar las configuraciones de la actual Ley General de Protección de Datos (LGPD) y los demás dispositivos. que tratan el tema. El objetivo es comprender la progresión de países y empresas nacionales e internacionales en la lucha contra las ciberamenazas, y las dinámicas para la búsqueda de la cooperación y la ciberdiplomacia bajo la perspectiva de la teoría realista. Se concluye que el proceso que dio origen a la LGPD fue fundamental para la unión de esfuerzos multisectoriales en Brasil, pero que se limitaron al ámbito doméstico, mientras que en la Unión Europea hay resultados satisfactorios en la proyección de la ciberseguridad como defensa. y herramienta de desarrollo, incluso así de lento, y focalizando los intereses nacionales sobre las decisiones colectivas.

Palabras clave: Protección de Datos; la seguridad cibernética; Ley General de Protección de Datos - LGPD; Reglamento General de Protección de Datos - RGPD; derecho a la privacidad; realismo

1 INTRODUÇÃO

A proteção de dados e o direito à privacidade se tornaram alguns dos maiores desafios da cibersegurança no século XXI. A necessidade de ação no combate às ameaças digitais exigiu dos países ações rápidas no tocante ao aperfeiçoamento da legislação, aparato técnico e tecnológico e cooperação internacional através da diplomacia (KELLO, 2018). A atividade cibernética cresceu exponencialmente nos últimos anos, principalmente após o acirramento da corrida comercial entre a China x Estados Unidos, e com o isolamento social provocado pela pandemia do COVID-19, que mudou as relações de trabalho, política e comércio, e migrou parte delas para o ciberespaço.

Apesar da tentativa em acompanhar a progressão da tecnologia digital, parte considerável dos países demonstrou pouca atenção na formulação de ações internacionais para validar as leis de proteção de dados e o combate de cibercrimes, e através da recusa para a cooperação, as leis que fundamentam o uso dos dados na internet permanecem sob o escopo dos estados de forma isolada, e em alguns casos, se aplicam a grupos de integração regional, como ocorre com a União Europeia.

Pela lógica, a cooperação, a ampliação da jurisdição internacional e a troca de conhecimento tecnológico seriam as formas mais adequadas de aprimorar o aparato de defesa cibernético dos países, além de garantir que o direito internacional tivesse maior amparo regionalmente e/ou mundialmente. Entretanto, a maioria dos países permaneceram com a ideia enraizada de adotar pensamentos unilateralistas e de competição inerente à anarquia internacional (WALTZ, Kenneth, 1979). Os estados percebem, na ideia realista, que a distribuição de tecnologia e de conhecimento estratégico poderia ser um maximizador do poder de seus adversários, gerando maior tensão nas relações internacionais entre os atores.

As Organizações Internacionais (OIs) apesar de fomentar uma ideia mais pautada no liberalismo, voltando a necessidade e o interesse da cooperação[1] para o sucesso do desenvolvimento, têm perdido força política pelas grandes potências, e passaram a atuar como coadjuvantes nas tomadas de decisão.[2]

O Brasil espelha sua agenda de segurança nos Estados Unidos no setor militar e na construção da política nacional de defesa. Em relação à cibersegurança, o processo não se difere

[1] São os quatro imperativos para a cooperação na teoria liberal: interdependência, transnacionalização, crescimento das instituições internacionais e a democracia (NYE, Joseph, 1998).

[2] BASRUR, R.; KLIEM, F. Covid-19 and international cooperation: IR paradigms at odds. SN Social Sciences, v. 1, n. 1, p. 7, 9 nov. 2020. https://link.springer.com/article/10.1007/s43545- 020-00006-4

tanto assim, pois os mecanismos legais de controle cibernético são hoje pautados nos costumes realistas também. Essa ideia é respaldada no entendimento de uma anarquia iminente e da necessidade de adoção do "*self help"* e do jogo de soma zero (KEOHANE; NYE, 1979). Apesar disso, o Brasil tem demonstrado atraso significativo na construção de mecanismos eficientes de defesa cibernética desde as primeiras leis que tratavam sobre o tema. A proteção digital está a passos largos de receber o mesmo empenho e investimento que há no campo militar, o que prova que este tema segue sem a atenção que deveria, gerando sérios riscos à segurança nacional e internacional em um futuro próximo.

Durante a segunda metade dos anos 1960 até o início dos anos 2000, pouco se registrou do empenho brasileiros em acordos cibernéticos com seus países vizinhos, encontros estes[3] que pautavam os estudos técnicos de cibersegurança para ampliar a ciberdiplomacia e a cooperação tecnológica nos territórios do cone sul, frente a ameaças domésticas e internacionais.

Com a criação da Lei Geral de Proteção de Dados, apesar de haver maior engajamento nacional pela formulação do conteúdo da lei de forma abrangente a todos os setores, o dinamismo da lei acabou por limitar o escopo de sua jurisdição a apenas o Brasil. Não obstante, a necessidade de aplicação de sanções internacionais para os cibercrimes têm limitado parte considerável do texto para tratar somente do controle de empresas nacionais e as relações comerciais e de direitos fundamentais. As singularidades dos atores e a complexidade do campo tecnológico colocam em evidência os limites do Direito na proteção digital, principalmente no que tange ao resguardo de dados e da privacidade em razão do *accountability*[4].

Diferentemente do caso latino americano, os 27 Estados-membros que compõem a União Europeia uniram esforços na construção de instituições especializadas no desenvolvimento de tecnologias para combater ciberameaças. Foi através do compartilhamento de informações e ampliação da jurisprudência que os países tentaram fazer valer o poder da lei cibernética do Regulamento Geral para a Proteção de Dados da UE. Considerando os aspectos naturais dos estados pela perspectiva realista, e pelos resultados registrados no progresso das

---

[3] O Brasil ocupava a 71ª colocação no ranking mundial de cibersegurança da ONU desde 2013. GOV.BR. Disponível em: <https://www.gov.br/gsi/pt-br/assuntos/dsi/noticias/2021/nova-posicao-do-brasil-no-ranking-de-ciberseguranca-da-onu>. Acesso em 15 nov. 2021.

[4] *Accountability:* Inexistência da autoridade suprema e a substituição do princípio da legalidade pelo princípio do pacta sunt servanda, fazem com que, na política internacional, as relações de poder dependam, em última instância, da capacidade de cada Estado para afirmar seus interesses perante os demais. No entendimento da política internacional, o respeito à soberania internacional limita o poder dos estados aos seus territórios.
JÚNIOR, Dimas P. *apud* (DAHL, 1997, p. 29).Um dado regime pode ser compreendido a partir desde a inexistência por completo de instrumentos de contestação e participação públicas até a realização por completo de condições para seu exercício, quando se chegaria a um dado estágio em que todos os protagonistas, representantes e representados, fossem reconhecidos como atores efetivos do espaço em vias de construção.

ações conjuntas, percebe-se que este processo se deu de forma impositiva pela necessidade de os países elevarem suas economias na Europa e expandirem a influência internacional frente à competição dos Estados Unidos x China e pelos conflitos regionais nas regiões vizinhas.

Este estudo tem por objetivo avaliar a construção da cibersegurança no Brasil, tendo como comparativo a legislação europeia. Para tal, percebe-se através de uma óptica realista a natureza das ações dos estados nas tomadas de decisão que competem à proteção de dados, o direito à privacidade e a diplomacia.

O realismo, apesar de ser uma das diversas agendas de RI que podem explicar os fenômenos internacionais sobre o tema, é a que melhor representa como a natureza dos atores desencadeará no futuro e prospecção da cibersegurança para o combate das novas ameaças cibernéticas. A evidência do comportamento egoísta dos estados permite que especialistas avaliem a necessidade de uma ação conjunta para aprimorar a rede de segurança mundial ao tempo que a ciberdiplomacia reduza os danos que as ciberameaças tendem a trazer para os países despreparados. Não menos importante, pode orientar os tomadores de decisão sobre o grau de cooperação que se pode esperar dos estados nas próximas políticas internacionais de amparo digital.

A pesquisa questiona quais são e como essas novas ameaças cibernéticas afetam a segurança dos estados, e como as instituições nacionais e internacionais têm agido para efetivar os esforços de criar uma rede global digital mais segura e em respeito aos direitos fundamentais democráticos. Ela analisa o processo internacional da construção da cibersegurança em um escopo internacional e avalia os cenários brasileiros e europeu. Desta análise, busca-se comparar como se desenvolveram os dois processos e quais as projeções dos resultados para o futuro nacional e internacional.

Conclui-se que apesar dos avanços na legislação brasileira em razão a criação da LGPD no Brasil, e do RGPD na União Europeia, em ambos os casos, são perceptíveis que a visão anárquica e egoísta dos estados perpassa a necessidade em juntar esforços mais amplos para combater os cibercrimes internacionalmente. Não obstante, há resultados positivos no campo doméstico brasileiro e europeu, principalmente nos últimos anos. Além disso, as Organizações Internacionais mediam a volta da cooperação cibernética para o futuro, voltando olhares para a sua necessidade urgente, mesmo que o jogo político segmente estas relações para que as grandes potências alcancem seus próprios interesses.

2 APONTAMENTOS GERAIS SOBRE A CONSTRUÇÃO DA CIBERSEGURANÇA E O DIREITO À PRIVACIDADE

Criada na segunda metade da década de 1960, a internet proporcionou mudanças significativas nas relações humanas e, consequentemente, na atuação do Direito quanto ao tratamento de pessoas, bens e serviços, em face da informação de dados. Alguns países perceberam a projeção da internet como potencial arma política, o que de fato veio a acontecer anos depois, quando os computadores ganharam popularização e tecnologias mais desenvolvidas (KELLO, 2018). Com a ampliação do número de usuários e a inovação das tecnologias dos computadores e celulares, a privacidade se tornaria cada vez mais discutida como um princípio questionável ou impossível de ser alcançado, diante da exposição excessiva de informações na internet e nos veículos de informação.

A privacidade se tornou direito em 1890, citada na obra *The Right to Privacy*, de Willes J., como direito ao isolamento. Neste século, as relações sociais não tinham o mesmo dinamismo que tem hoje em dia, e as informações não veiculavam com tamanha rapidez e projeção. A ideia de "isolamento" era, nesta época, entendida como o direito total sobre colocar-se à parte, seja da sociedade, ou de determinado local. Percebendo-se hoje a impossibilidade do ser humano de se retirar completamente no ambiente digital, configura-se a seguinte pergunta: "como é visto esse direito ao isolamento em uma sociedade em que a inserção digital é primordial nas relações de trabalho, no campo social e econômico? ".

Este debate não se baseia mais no conceito de isolamento em seu sentido literal devido a incapacidade que a internet impõe sobre os dados, mas compreende-se nela que a privacidade deve existir sobre o controle à titularidade das informações dos usuários em qualquer momento, garantido pelas leis, e respeitando os limites que configuram os direitos fundamentais. Sob a esfera internacional, onde os estados e as instituições são os atores analisados, segundo a ótica neorealista de Kenneth Waltz (1979), mas sob uma roupagem sistêmica de política externa (Ripsman *et al*, 2016), entende-se que as informações podem e são usadas como estratégias de maximização do poder dos atores, e em uma balança de poder onde os estados buscam os interesses nacionais, não haveria, senão por ameaça ao *status quo*, a cooperação pelo resguardo internacional deste direito.

As variadas formas de inserção tecnológica no Brasil e em todo o mundo foram se sofisticando durante os anos em caráter dos interesses das grandes empresas em conjunto à demanda social por conectar-se de forma simples e instantânea com a rede mundial, além da competição internacional acirrada por mercados potenciais. Essa inserção conduziu à revolução

da comunicação social e comercial, que teve diversas fases, mas que se consolidou na sociedade tecnológica que vigora até hoje.[5]

A democratização do acesso à internet proporcionou aos países maior controle sobre as informações e a vigilância de suas populações. Porém, emergiram questões sobre até onde poderia chegar este controle dos dados prestados e quem mais teria acesso a eles. Isso ocorreu em parte pelos escândalos envolvendo vazamento de informações sensíveis por falha técnicas e também pelo vácuo de poder institucional que subsiste na esfera da segurança da informação.

Nas relações interpessoais, as redes sociais e e-mails ganharam notoriedade e ajudaram a popularizar a internet ao redor do globo, devido à capacidade de conectar pessoas em tempo real. Apesar da promessa de um mundo mais prático, não tardou para que houvesse também ameaças à normalidade dos serviços online e à garantia da proteção dos dados de usuários, que consequentemente ampliaram este debate para a esfera do direito à privacidade e do direito à propriedade.

Domesticamente, a constante ameaça aos direitos fundamentais exigiu das esferas públicas resposta que garantisse um controle maior sobre as atividades cibernéticas, permitindo aos usuários o direito de resguardar suas informações frente àqueles não autorizados, o que, por sua vez, amplia a necessidade da capacitação tecnológica dos países para realizar este controle efetivamente.

No Brasil, definiram-se mecanismos jurídicos para o controle da atividade cibernética em relação à legitimidade e ao controle da atuação do meio digital na economia, relações internacionais e também no que compete ao direito civil e criminal através do Marco Civil da Internet (Lei 12.965/2014), a Lei dos Crimes Cibernéticos (Lei 12.737/2012), conhecida como Lei Carolina Dieckmann e da Lei Geral de Proteção de Dados (Lei nº 13.709/2018). Não foi sempre que o país esteve resguardado de tal proteção jurídica para crimes cibernéticos, então a legislação brasileira atuava a partir da compreensão dos crimes tipificados pelo seu teor, e não pelo ambiente em que ocorriam. Nestes casos, era utilizada a compreensão da violação de princípios legais do Código Penal e da Constituição Federal de 1988. Em relação à invasão da privacidade, considerava-se o direito à privacidade, resguardados pelo Artigo 5º.

Apesar da boa fé destes mecanismos, foi com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) que o Brasil finalmente tratou com solidez a seguridade dos dados pessoais, antes sem jurisdição efetiva. Segundo Bruno Bioni:

---

[5] LIMA, Paulo *et al*. Marx como referencial para análise de relações entre ciência, tecnologia e sociedade. Ciência & Educação (Bauru) [online]. 2014, v. 20, n. 1. Acesso em 15 out 2021, pp. 175-194. Disponível em: <https://doi.org/10.1590/1516-731320140010011>

> A LGPD é a primeira lei no Brasil a tratar de modo sistemático e coerente a proteção de dados pessoais, definindo regras e procedimentos estruturantes dessa nascente área do direito, o que terá grande impacto na vida das pessoas, das empresas e dos entes dos setores público e privado, de modo geral. (BIONI, 2021, p.6).

A LGPD teve importante papel no desenvolvimento de políticas de controle do conteúdo armazenado, compartilhado e vendido a terceiros, pois, sob a ótica de segurança nacional e internacional, a ameaça do ambiente digital se torna cada vez mais inevitável.

No panorama internacional, é possível perceber que a tecnologia do espaço digital se tornaria uma arma político-econômica na balança de poder, sendo citada por Lucas Kello (2018, p. 3), que diz que "apesar das características peculiares da segurança em nossos tempos, a tendência dos especialistas em relações internacionais tem sido trazer a arma virtual à regra da política convencional para negar a existência da revolução cibernética".[6]

Na Europa, surge em 2016 o Regulamento Geral sobre a Proteção de Dados 2016/679, que inspirou a LGPD no Brasil e incentivou outros países a fortalecer seus aparatos de proteção cibernética. Com esta ferramenta, as atividades na esfera da União Europeia e do espaço econômico europeu puderam inovar na segurança internacional, pois seu ordenamento jurídico se ampliava para fora do ambiente doméstico de cada país, estendendo-se para a esfera de toda a União Europeia. Nesta perspectiva os estados-membros poderiam pensar em conjunto sobre o aperfeiçoamento, mudanças na legislação e sobre os limites técnicos e jurídicos para a prevalência deste novo instrumento.

Os resultados desse modelo de proteção são tidos como promissores em razão da qualidade de seu conteúdo, da efetividade da regulação, e da validação de autoridade responsável por averiguar e controlar a ação das empresas e evitar excessos das partes.

Contextualizando as percepções das ameaças digitais, entende-se a importância em caracterizar historicamente a evolução da invasão de dados. Este fenômeno começou pouco após a popularização dos computadores particulares, e foi desenvolvido e alimentado por grupos de *crackers* e empresas que investem cada vez mais na busca pelo aperfeiçoamento em traçar o perfil individual, indicando para seu fim a intenção de melhorar a experiência do usuário, e que, ao longo dos anos, mostrou-se muito lucrativa. Porém, e ao mesmo tempo,

[6] Na perspectiva da segurança internacional, Kello aborda em *The Virtual Weapon and International Order* (2017) a desmistificação da cibersegurança como um tema meramente limitado ao ambiente digital. A revolução cibernética aponta que questões de soberania estatal são ainda vigentes com a ciber-soberania (cyber-sovereignty gap), e que as grandes potências utilizam deste cenário para ampliar seu escopo de manutenção do poder em face das ameaças internacionais e utilizam dessas ferramentas para controlar demais países. Além disso, o autor critica a visão tradicionalista que exclui o tema cibernético das pautas de defesa, tornando a incitar que os estudos teóricos devem ser aplicados à realidade vigente, e que há uma enorme necessidade dos países em investir na proteção contra estes novos riscos.

rendeu diversos processos para grandes empresas por seu caráter massivo e influenciador na tomada de decisões, como ocorreu nas eleições presidenciais dos Estados Unidos, em 2016, e nas eleições brasileiras de 2018.

A invasão de dados e da privacidade na internet se popularizou no início dos anos 2000, com a venda de programas de spam[7] fornecidos por diversos sistemas de banco de dados de sites diversos, que vendiam ou compartilhavam informações de *big data*.[8] A desmistificação das manobras tecnológicas com que empresas buscam captar usuários sem que haja interesse dos mesmos suscitou o debate sobre a licitude destas ações, seja da empresa que vende estas informações, seja pelo receptor, que as utiliza sem consentimento prévio. A violação do contrato e da privacidade é expresso na CF, que traz em seu artigo 5º, inciso X: "São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação."

Não obstante, o aperfeiçoamento das máquinas na construção de perfis cada vez mais sofisticados sobre seus usuários instiga atrair pessoas para suas plataformas, aumentar o tempo de uso, incentivar a utilização de programas e sites parceiros para vender produtos, ampliando sua interatividade e tornando os usuários produtos rentáveis para a empresa.[9]

Apesar de não haver objeções em relação à concorrência e às táticas de captação de clientes na internet, desde que respeitando os termos de cada contrato, há em diversos casos a ilicitude no real manuseio das informações prestadas pelos usuários e negligência quanto à sua proteção e intimidade. Em um mercado de tendência liberal, a intervenção estatal colide com os interesses do livre mercado, mas o descontrole da ação de criminosos frente à segurança doméstica e internacional exige que os estados nacionais tomem medidas sobre o tema.

---

[7] RIBEIRO, Gabriel F. Uma das opções usadas por spammers é a compra de banco de dados de usuários em sites ou serviços. Mas quem manda spam também produz suas próprias listas, obtidas seja pelos chamados "ataques de dicionários". **TILT UOL**. São Paulo, 2018. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2021/08/29/quem-sao-os-culpados-pelo-spam-que-atormenta-o-seu-e-mail.htm?cmpid>. Acesso em 21 set. 2021.

[8] Com o desenvolvimento da inteligência artificial, são utilizadas variáveis que aperfeiçoam cada vez mais na busca por clientes em potencial, através de combinações matemáticas feitas pelos computadores, que identificam o perfil do cliente através das informações fornecidas por estes em sites, através de *cookies*, *ransomware*, e de outros sistemas complexos. Ver: **Vazamento e roubo de dados**: como acontecem e como se precaver. Disponível em: <https://chcadvocacia.adv.br/blog/vazamento-de-dados/2021>. Acesso em 28 set. 2021.

[9] Carlos Affonso (2019) indica que a violação de dados ultrapassa os limites contratuais de uso das ferramentas e sites na internet. A experiência com a proteção da privacidade se choca com o interesse comum em fazer parte da comunidade global tecnológica. A experiência do usuário passou a criar uma persona de seus usuários, utilizando das informações de seus usuários, muitas vezes em troca do serviço "gratuito" de sua plataforma, que disfarça o fato que os usuários passam a ser o produto vendido. O palestrante afirma que: "Se você não estiver pagando por um determinado produto, o produto pode ser você" 8min45seg. *In*: **Privacidade e Proteção de Dados no Brasil**. Carlos Affonso Souza. TEDxPetrópolis. Disponível em: <https://www.youtube.com/watch?v=Zau-x-j_Uu8>.

Um dos pontos que a Lei Geral de Proteção de Dados e o Regulamento Geral sobre a Proteção de Dados defende é o controle sobre eventuais excessos da invasão da privacidade pelas empresas, pois até o momento anterior a estas leis, não haviam regras explícitas sobre o abuso e excesso de informações de seus clientes.

Em razão ao que prevê o armazenamento único e exclusivo de informações relevantes para o uso dos serviços desses sites e aplicativos, as informações como localização, tempo de uso do aplicativo, interesses e mudança de gostos e a informações bancárias ganharam atenção maior no tocante à impossibilidade de serem transpassadas a outros sem autorização prévia. Com os governos não é tão diferente. Em uma percepção ampliada do quadro da segurança dos países, o armazenamento de informações sensíveis sobre sua população é por um lado positiva no controle estatal, e por outra, uma arma que pode se voltar contra o próprio país (HUREL, 2020). O controle de dados pelas autoridades e órgãos nacionais deve se atentar no uso correto das informações, e deve dar maior atenção aos setores onde pouco se investe na construção da defesa cibernética e na capacitação técnica de seus funcionários.

No Brasil, a tardia implantação de uma agência de controle cibernético fez com que a atividade circulante de dados chegasse a níveis consideráveis, e mesmo após a sanção da nova lei, já se notam os desafios que a autoridade geral de dados deve enfrentar.

A proteção de dados privados e públicos interessa, e a LGPD como ferramenta de controle de excessos permite evitar que as empresas se tornem portadoras das informações prestadas para o uso de seus serviços, visando à condição pareto-ótima. Por outro lado, cresce também um desafio que complica a efetividade dos esforços nacionais e internacionais: a desinformação, principalmente através de *fake news*.

Tendo em vista a pouca atenção dada pela cibersegurança durante o início do século XXI,[10], os esforços atuais para criar pilares de sustentação das agências de combate ao excesso de inviolabilidades do meio digital não conseguem acompanhar os novos desafios, devido à complexa ampliação da inserção tecnológica e do aperfeiçoamento da inteligência artificial.

3 DESENVOLVIMENTO DAS AGENDAS E COMISSÕES DE SEGURANÇA CIBERNÉTICA (BRASIL E EUROPA)

[10] BRAUN, Daniela. “Em média, 46% das empresas brasileiras investem até US $1 milhão por ano em cibersegurança. A mesma faixa de investimentos à segurança é dedicada por uma parcela bem menor (21%, em média) das empresas de Cingapura e os membros do G7 (Alemanha, Canadá, Estados Unidos, França, Itália, Japão e Reino Unido), já que boa parte de seus orçamentos em proteção de sistemas estão na faixa de US$ 1 milhão a US$ 5 milhões anuais.” **Valor Econômico**. São Paulo, 2021. Disponível em: <https://valor.globo.com/empresas/noticia/2021/09/06/no-brasil-ciberseguranca-e-vista-como-gasto-e-suporte.ghtml>. Acesso em 21 set. 2021.

Com a eclosão do uso de dispositivos eletrônicos com acesso à internet em diversos setores, o mercado digital se expandiu no século XXI de forma jamais vista, atingindo no Brasil cerca de 2 dispositivos por habitante (FGV cia, 2021) e a marca total de 5,22 bilhões de usuários no mundo.[11] Consolida-se a ideia de que o aumento do número de pessoas conectadas à rede gerou consequentemente aumento nas denúncias por crimes cibernéticos e também maior participação da sociedade na formulação das regras e limites sobre a atuação dos Estado e de empresas no controle e manuseio das informações.

Em razão da ameaça não se limitar ao campo doméstico, muitos governos aproveitaram este gancho para aprimorar os recursos de proteção de dados para fins de resguardo da segurança nacional e de seus interesses privados, tendo em vista que parte considerável dos ataques *hackers* à instituições públicas e federais vinham de outros países. Segundo a vertente Realista da Teoria de Relações Internacionais, a função primeira do Estado é manter-se enquanto Estado num mundo cujas relações de força e dimensões de Poder não devem ser desprezadas, pelo contrário, devendo ser realçadas quando da análise. (ACÁCIO, Igor; SOUZA, Gills. 2012, p.7)

A história da evolução da tecnologia digital tem marco inicial após a eclosão da Guerra Fria em 1945, quando os Estados Unidos criaram a internet com o propósito de interligar laboratórios de pesquisa, e que a partir da corrida armamentista e tecnológica, sucedeu à revolução da informação, que perdura até os dias atuais. Tendo em vista a capacidade estratégica da internet e da informação como arma, organizações, pessoas e até mesmo estados utilizam deste artifício como forma resguardada este *soft power*[12].

Em suma, a internet proporcionou na mudança significativa de várias formas de interação humana, pois acelerou o progresso desenvolvimentista, o acesso à informação e ampliou a disputa entre os atores do sistema internacional.

---

[11] Nota-se que o dado é referente a fevereiro de 2021. Com a projeção do mercado tecnológico para atividades home-office devido à pandemia do coronavírus, projeta-se que este número seja ainda maior. **Istoé Dinheiro**, 2021. ed. nº 1243 08.10. Disponível em: <https://www.istoedinheiro.com.br/numero-de-usuarios-de-internet-no-mundo-chega-aos-466-bilhoes/>. Acesso em 10 set. 2021.

[12] NYE, Harvard Joseph. *Soft Power* é conceituado na teoria das Relações Internacionais como uma habilidade de influenciar o comportamento de outro através da cultura e ideologia, geralmente utilizada pelos Estados. Soft Power: *The Means to Success in World Politics* (2004).
Em um contexto aplicado à internet, é associado o *soft power* à informação e inteligência artificial dotados da capacidade de influenciar o comportamento humano e ideologia através do molde que a internet passa a definir sobre as informações já obtidas dos usuários ou da exposição massiva de informações relacionadas a determinada temática.

Sendo utilizada também como ferramenta de controle ou privilégio de informações em um mercado estritamente competitivo, abriu-se neste espaço portas para o empreendedorismo por meio dos vazios institucionais (*institutional voids*)[13], maior cooperação internacional, ampliação dos sistemas de segurança nacional, além de gerar visibilidade para países antes ignorados no sistema internacional.

Apesar da aproximação das massas com as redes sociais e da redução das dificuldades de se conectar, a internet e seus mecanismos trouxeram consigo também os conflitos e desafios atrelados à segurança dos dados e a invasão da privacidade, que passaram a abranger a utilização dos meios digitais para coagir o pensamento político, social e econômico, além de diversos outros problemas.

Na Europa já se pensava na progressão de ameaças que viriam a impactar a ordem internacional e as relações internacionais entre os países e seus respectivos blocos econômicos, e pelo indício do abalo nas estruturas comerciais e políticas na União Europeia, os países membros alcançaram consenso para criar o Regulamento Geral sobre a Proteção de Dados - RGPD 2016/679. Este processo, por sua vez, caminhou lentamente, pois os estados-membros avaliavam neste desafio as intenções e possibilidade de ação de seus aliados em um futuro conflito pela detenção de mercados e de tecnologia, e que discutem até o tempo presente[14].

O processo de efetivação dos esforços conjuntos na construção de um dispositivo brasileiro bem consolidado adveio de diversos interesses particulares sobre pontuações específicas da lei, mas que concordavam entre si no tocante à necessidade do controle administrativo do tratamento dos dados veiculados pela internet, uma vez que, até então, não havia amparo estatal. Este processo durou cerca de 8 anos para que, finalmente em 2018, a Lei nº 13.709/2018, conhecida como a Lei Geral de Proteção de Dados, entrasse em vigor.

Deste processo averígua-se as leis anteriores que deram origem à LGPD, e segundo Biasi (2021) foram diversos os dispositivos nacionais e internacionais que influenciaram no seu texto e conteúdo. Não obstante, a ideia de uma lei abrangente sobre o conteúdo digital já era discutida em fóruns internacionais, apesar que:

> Esta ideia só ganhou maior tração a partir de meados dos anos 2000, com a participação do Brasil em negociações internas do Mercosul, foro que abrigou

[13] KHANNA, Tarun. O fator mais importante em uma economia de mercado é a capacidade dos compradores e vendedores de se encontrarem e concluir as transações da maneira mais perfeita possível. Os vazios institucionais são as lacunas que existem em mercados específicos que servem como barreiras para as interações e transações ideais de compradores e vendedores. *Entrepreneurship in Emerging Economies.* **Harvardx**, 2021 edX Inc.

[14] BOSE, Nandita. "EUA e UE vão discutir regulação conjunta de gigantes de tecnologia em encontro". CNN Brasil. 2021. Disponível em: <https://www.telesintese.com.br/comissaria-da-ue-defende-regulacao-de-competicao-mais-abrangente-para-big-techs/>. Acesso em 11 nov. 2021.

> movimentos de pressão, por parte de países como a Argentina, para a construção de uma norma comum aos países do bloco. Embora nunca se tenha concretizado a ideia de uma regulação de proteção de dados para todos os países integrantes do Mercosul, os debates deflagrados por essa proposta serviram de combustível para a internalização do tema pelo Poder Executivo brasileiro. (BIONI, p. 21, 2021)

Seja no cenário europeu ou no brasileiro, foi defendido o reconhecimento da proteção de dados como direito fundamental, reafirmando-se a ideia de que a segurança da informação e a privacidade importam mesmo em sites ou aplicativos, dentro ou fora dos limites fronteiriços dos países.

Para melhor descrever o processo de criação das agendas e as comissões que sucederam na LGPD e no RGPD, dividiremos a explanação em duas sessões. Na primeira, introduz brevemente os acontecimentos; em seguida, procede-se a comparação do conteúdo destes dispositivos e apresenta-se uma projeção de seus efeitos em situações contempladas em cenários em que pode haver deficiência ou vício destas leis.

3.1 União Europeia: Comissão de Segurança Cibernética e o RGPD

A União Europeia desenvolveu seu aparato de defesa cibernética de forma mais abrangente que o Brasil, desde o seu teor quanto aos esforços mediados para que houvesse uma ação conjunta dos países em relação à proteção de dados e segurança internacional. No entendimento neorealista, a percepção da UE sobre a projeção da ameaça cibernética se configura rapidamente, e a cooperação, mesmo que forçada, exigiu a ação mais precocemente na Europa. Segundo Clarke e Knake: "A guerra cibernética é global. Em qualquer conflito, os ataques cibernéticos rapidamente se tornam globais, à medida que computadores e servidores adquiridos ou hackeados secretamente em todo o mundo são colocados em serviço. (2010, pp. 30-31).

Marcada por diversos conflitos de interesses entre durante a história europeia contemporânea, o interesse na proteção de suas informações e o controle estratégico foram difundidos para além das pautas de defesa militar. O tema da cibersegurança se tornou cada vez mais reconhecido como necessidade dos países no alcance da paz e da ordem, pois para muitos a cibersegurança era vista como uma ferramenta política e econômico-estratégica. (KELLO, 2017).

O Conselho Europeu é uma instituição da União Europeia de natureza política criada através dos artigos 235° e 236° do Tratado sobre o Funcionamento da União Europeia - TFUE, que, com base no avanço da ameaça do ciberterrorismo e da tensão gerada pelos ataques

cibernéticos, entrou em 2016 em acordo para construir conjuntamente medidas para o combate dos crimes cibernéticos no espaço digital.

Com a iniciativa da justiça da União Europeia, definiram-se os pontos necessários para que houvesse efetividade do controle de atividades cibernéticas entre os países membros através da cooperação, visando o aprimoramento das instituições e do texto penal acerca da punição e autuação das atividades ilícitas e a criação de estratégias de combate e previsão.

Sustenta-se no final do ano seguinte o esforço e aprimoramento da ação conjunta internacional entre os países membros para alavancar resultados satisfatórios sobre o combate dos ciberataques e de garantir maior eficiência das agências de controle das atividades cibernéticas e permitir respostas coordenadas.

Por meio de um acordo interinstitucional, foi criada uma Equipe de Resposta a Emergências Informáticas - CERT-UE, de caráter permanente, que abrange todas as instituições e agências da UE. (Conselho da União Europeia, 2021). Tal resposta foi viabilizada após o acordo para a instauração do plano de ação para o combate de crimes cibernéticos na UE, que garantia a proteção digital como um direito. A sociedade civil europeia e os próprios países forçaram o Conselho Europeu a adotar medidas rápidas, tendo em vista os índices de crescimento de invasão de dados no território, e a diminuição da confiança depositada nestes países no campo econômico-comercial.

Em 2018 foram apresentados, pelo Conselho Europeu, projetos de controle dos ataques cibernéticos devido ao desenfreado aumento dos ataques à proteção de dados de cidadãos e dos bancos de dados dos governos.[15] Esta iniciativa tinha como intuito demonstrar o empenho e força da cooperação europeia em face do abuso de hackers, projetando internacionalmente a necessidade que os blocos econômicos e agências internacionais deveriam aperfeiçoar seus mecanismos jurídicos em conjunto. De acordo com Gabriella França (2020):

> Apesar dos resultados satisfatórios, é importante ressaltar que a elaboração de políticas estratégicas ainda tem uma perspectiva muito centrada no Estado o que impacta nas decisões relacionadas à segurança do ciberespaço, ainda que seja uma matéria de natureza transfronteiriça. (*apud* BELÁZ 2019, p. 17)

A ideia principal destes projetos era diminuir os avanços das ciberameaças, difundindo a ideia de um ciberespaço mundial, aberto, livre, estável e seguro, no qual se aplicam inteiramente os direitos humanos, as liberdades fundamentais e o Estado de direito. (Conselho da União Europeia, 2021).

---

[15] Ciberataques custaram US $45 bilhões em 2018. Segundo um estudo, se o número de ataques deste tipo caiu 20% em relação a 2017, as perdas financeiras aumentaram 60%. AFP Agence France-Presse, **Exame**, 2019. Disponível em: https://exame.com/tecnologia/ciberataques-custaram-us-45-bilhoes-em-2018/>. Acesso em 01 set. 2021.

No mesmo ano foi concretizado o Regulamento Cibersegurança, oriundo das negociações do Conselho com o Parlamento Europeu, que incentivava os reforços da adaptação às novas ameaças previstas no campo digital.

O documento compromete as partes a garantir a certificação estabelecida pela União Europeia para todas as atividades vinculadas à internet, além de aprimorar a agência intitulada *The European Union Agency for Cybersecurity* - ENISA. Com o perigo deste regulamento falhar, exigiu-se o preparo das agências de proteção cibernética para além do combate de assuntos cibernéticos caracterizados como ciberataques, o que resultou na reestruturação do plano de ação desta agência[16]

A nova estratégia adotada, e que viabilizou a criação do Quadro Estratégico da UE para a Ciberdefesa ordenou as prioridades do Conselho Europeu para estudar e definir os temas em que as agencias passariam a ser responsáveis, a fim de otimizar os resultados pretendidos e evitar sobrecarga destas instituições.

Deste processo se origina a agência permanente da União Europeia para Cibersegurança, criada por este grupo de países juntamente a esforços diplomáticos, garantindo que as relações entre empresas e usuários fossem mais transparentes e asseverando o direito da pretensão por parte destes usuários, quando lhes aplicados prejuízos.

Com os diversos processos anteriormente descritos e a cooperação entre os países membros da União Europeia, o Regulamento Geral sobre a Proteção de Dados, que havia sido aprovado em 2016, finalmente entraria em vigor, dois anos depois.

O RGPD facilitou a ação dos estados em compreender os novos desafios cibernéticos em ação conjunta com o Parlamento Europeu, em duas iniciativas: a criação de uma base de conhecimentos de excelência em matéria de cibersegurança – que seria o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a criação de uma Rede de Centros Nacionais de Coordenação. (Conselho da União Europeia, 2021).

Através do esforço projetado para a efetivação do RGPD, foi criado o Regulamento Cibersegurança, que substituiu a ENISA por uma nova agência mais preparada e especializada sobre os assuntos acordados pelo Conselho Europeu. Posteriormente, o RC ganhou respaldo para autuar empresas, indivíduos e países que conferissem prejuízos originados de ciberataques aos membros da União Europeia, e que espelhou também nos objetivos buscados pelo Brasil

[16] Conselho da União Europeia. A ENISA contribui para a elaboração da política e da legislação da UE em matéria de segurança das redes e da informação e, por conseguinte, para o crescimento económico no mercado interno europeu, e passou a legislar sobre ameaças de natureza química, biológica, radiológica e nuclear (QBRN). 2021. Disponível em: <https://europa.eu/european-union/about-eu/agencies/enisa_pt>. Acesso em 02 set. 2021.

para fortalecer seu aparato de segurança tecnológica. No espelho realista, os constantes processos de aprimoramento das agências de proteção cibernética tinham além do intuito de aprimorar a defesa, fortalecer a visibilidade e o poder da UE regionalmente e mundialmente.

A inovação neste cenário por parte da UE é perceptível pelo reconhecimento internacional e regional que as agências de proteção cibernética passam a ter. Sobre a ideia defendida do respeito à soberania dos Estados, a força coercitiva do grupo e a ideia respaldada de ações necessárias para a proteção cibernética em âmbito internacional garante o funcionamento mais assertivo em suas ações.

Com o avanço iminente da tecnologia e da internet no campo político e econômico internacional, diversos países passaram a repensar a segurança de dados, considerando estratégias comerciais para ampliar seus mercados, visto que se expandiram através dos bancos digitais, serviços de investimento e as criptomoedas. Nesta estratégia estão inseridos também fatores como velocidade de dados e da informação que ganharam importância na Europa e no mundo com os avanços da tecnologia 5G, a qual tornou-se importante para a projeção e manutenção das atividades econômicas e sociais na União Europeia.

Mais uma vez o Conselho Europeu reivindica a atenção dos Estados-membros para a adoção de medidas conscientes e inovadoras para combater as ameaças cibernéticas no ano de 2020. Através destas problemáticas, o Parlamento e o Conselho pretendiam combater a desinformação ostensiva, gerada pelo aumento de usuários conectados pela rede, influenciada em parte pelo isolamento social causado pela disseminação da Covid-19. Mesmo bem sucedida em situações de amparo tecnológico da covid, Rajesh Basrur e Frederick Kliem induziram que:

> A OMS, como única organização global de saúde pública de magnitude, permaneceu relativamente ineficaz devido às prioridades conflitantes de seus membros. E mesmo a União Europeia (UE) e a Associação das Nações do Sudeste Asiático (ASEAN) foram constrangidas por surtos de nacionalismo e reações instintivas unilaterais. (BASRUR; KLIEM, 2021, p.7).

Isso demonstra que mesmo em casos em que a cooperação internacional é necessária, os países voltam os esforços apenas para as situações em que lhes é exigida determinada conduta cooperativa e de ganhos (WALTZ, 1979, adaptado para o contexto).

Um dos maiores avanços na proteção de dados e da privacidade dos cidadãos europeus e empresas, a estratégia de cibersegurança da UE, fomenta a inovação e novas alternativas técnicas e científicas para garantir a democracia digital e a segurança dos usuários na rede. Prevê, inclusive, a promoção de ações que visem o desenvolvimento social, ambiental e tecnológico em escala internacional, com amparo em valores compartilhados do direito internacional e das *jus cogens*.

Nesta mesma direção, o Parlamento Europeu buscou utilizar sua influência e força política para, junto a outros atores coordenados, trazer o foco das agências de proteção cibernética para o combate do ciberterrorismo e à exploração de crianças e jovens. Instou as agências a empreender ações para detectar, remover e denunciar abusos sexuais de crianças, alcançando também o combate ao aliciamento, isto até que entre em vigor a legislação permanente anunciada pela Comissão Europeia. (Conselho da União Europeia, 2021).

Prospectando o futuro digital, o CE passou a estabelecer metas para a melhoria da capacidade de atuação das instituições, prevendo que a informação, o aparato tecnológico e a especialização de profissionais proporcionam resultados benéficos para o desenvolvimento da Europa. Dentre os fatores que são influenciados pela evolução dos fatores citados, a resiliência e o combate da desinformação e a implantação da internet 5G se tornaram os objetivos mais prospectados para os próximos anos.

Tabela 1: Construção da proteção cibernética na União Europeia -UE

Fonte: BRAGA, Noelson, 2021.

O crescimento europeu foi proporcionado em parte pela inovação e pela ampliação da legislação para tratar da proteção de dados e democratizar seu acesso (Índice Global de Inovação de 2021). Em 2021, foi sancionado o projeto que prevê aumento exponencial da economia europeia para os próximos quatro anos.

Enquanto no Brasil se espera o prazo de adequação das empresas para reforçar seu aparato de defesa cibernética, a Europa já vislumbra o combate aos cibercrimes na realidade. Apesar de ser um período ainda instável e incerto no que se refere ao sucesso dessas iniciativas, o caráter inovador da cooperação europeia se reflete no progresso que os brasileiros esperam da Lei Geral de Proteção de Dados, que está aliada à CF de 1988, ao Código de Defesa do Consumidor e aos demais instrumentos jurídicos em seu favor.

3.2 Brasil: Relatório de defesa e a LGPD

Com cerca de 212 milhões de habitantes, o Brasil detém hoje a 6ª maior população no mundo. Diante deste fato e, tendo em vista a construção histórico-política brasileira, foi necessário que se adotasse uma Constituição Federal robusta e apta a atender as demandas por soberania popular, garantindo os seus direitos, deveres e a segurança nacional[17].

A preservação do direito à segurança de dados e da privacidade de pessoas físicas e jurídicas passou a ganhar destaque nas últimas décadas, principalmente pela ascensão da internet como meio de comunicação e pela rápida transmissão de dados.

Apesar destas evoluções, a informação se torna cada vez mais acessível a terceiros; estes, por sua vez, podem utilizá-la de má fé para extrair lucros diante da venda, reprodução ou aplicação de dados em diversos tipos de golpes envolvendo a invasão da intimidade e o acesso a informações pessoais.

Para dar maior vigor à Constituição Federal de 1988, foram criados outros mecanismos jurídicos que atendessem especificamente a seara do direito da personalidade, abrangendo os campos físico e o digital. Não obstante, discute-se hoje os limites das leis vigentes e o próprio direito brasileiro, tendo recentemente se avaliado que nem mesmo as instituições públicas têm um controle efetivo sobre a cibersegurança: ainda se busca compreender como foi possível o vazamento dos dados de 223 milhões de brasileiros por um grupo de hackers.[18]

Nas tentativas do poder público brasileiro em validar os diversos mecanismos jurídicos de proteção cibernética, o conteúdo da Lei Geral de Proteção de Dados (LGPD), a Constituição Federal de 1988 e o Código Civil são utilizados de forma simultânea para fortalecer o direito de pretensão sobre os dados e o direito à privacidade.

A notícia do vazamento, datada de 22 de janeiro de 2021, gerou enorme discussão popular e também no âmbito jurídico, pois, até os dias atuais, são poucos os mecanismos de

---

[17] Carlos Ayres Britto afirma que o texto é um dos melhores do mundo. "Essa Constituição nos torna um país juridicamente primeiro-mundista. "Se temos andado mal das pernas é porque temos andado de costas para esta Constituição. **TV SENADO**. Disponível em: <https://www12.senado.leg.br/noticias/materias/2018/08/02/constituicao-brasileira-e-de-pais-de-primeiro-mundo-diz-ayres-britto>.

[18] Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. **G1 Economia,** 2021. Os dados vazados abrangiam pessoas vivas e mortas no país, sendo matéria estudada pela LGPD, mas que está fora dos limites de sua ação jurídica por ter ocorrido antes de seu período de vigência. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml>.

penalização e proteção dos dados e, dada a amplitude do campo cibernético, é quase impossível gerenciá-los.

A empresa PSafe foi quem identificou o vazamento em massa de dados de milhões de brasileiros para download na internet. Espanta o fato de o número de pessoas que tiveram seus dados vazados ser maior que a própria população do país. Avalia-se que dentre os dados expostos, existem informações de falecidos também. Dentre os materiais expostos estão: dados bancários de diferentes bancos, CPFs, endereços, fotos de perfil de redes sociais como o *LinkedIn,* etc.

Para autuar e inibir tais ações, a Polícia Civil, especializada em crimes cibernéticos, é quem trata do caso por solicitação da Autoridade Nacional de Proteção de Dados - ANPD. A LGPD seria a ferramenta mais bem organizada, no momento, para tratar o caso, tendo em vista seu escopo e o poder coercitivo punitivo; porém, deve-se tomar em conta que a mesma ainda se encontra em fase experimental, dado o seu curto tempo de vigência.

É compreensivo que os esforços dos agentes de proteção de dados não tenham obtido resultados tão satisfatórios até o momento, devido a criação desta lei ter ocorrido, de fato, somente em 2021. O argumento aqui é que as tentativas de combater as ameaças digitais precisam ser primeiramente elencadas e estudadas para oferecer maior entendimento das falhas deste processo.

No que tange à construção da legislação referente ao texto da LGPD e à sua aprovação, observa-se condicionantes que permitiram o alinhamento de diferentes frentes no arranjo dos princípios que a lei iria apontar, como o Manifesto pela Aprovação da Lei de Proteção de Dados Pessoais em julho de 2018, o qual, segundo Bioni:

> Nessa ocasião, 80 (oitenta) signatários, a ampla maioria entidades, reuniram-se em torno de um objetivo comum: pressionar o Senado Federal pela aprovação do então Projeto de Lei da Câmara nº 5311, que veio a se tornar a Lei nº 13.709/2018. O grupo era diverso, composto por empresas de diferentes ramos, pesquisadores, entidades do terceiro setor e até órgãos públicos, como Procons. (2021, p. 19)

Esta coalizão de interesses resultou na aprovação da Lei Geral de Proteção de Dados, o que é indiscutível; mas é importante destacar que seu início não surgiu do simples acordo das partes anteriormente citadas. Cada grupo tinha como objetivo preservar e promover seus interesses privados, mas coincidiram no teor da necessidade de embasar uma lei forte no quesito da proteção de dados segundo a esfera do direito brasileiro.

Foi ao longo percurso de importantes regras e leis que a LGPD ganhou em seu texto pontos tão significativos para a proteção de dados, como o Código de Defesa do Consumidor,

de 1990, o qual fortalece a disciplina nas relações do setor privado com seus consumidores, e que recentemente serve de instrumento auxiliador da nova lei para a questão da validade da segurança de dados e da punição em casos de desobediência pelas empresas.[19]

Outro instrumento que teve grande importância para a efetividade da Lei Geral de Proteção de Dados no Brasil foi a Lei nº 12.414/2011 (Lei do Cadastro Positivo)[20], que vem debatendo com o processo de funcionamento do projeto de aplicação do *Open Banking*, que implica no compartilhamento de dados bancários de usuários entre diferentes instituições financeiras, com a permissão prévia dos clientes titulares dos dados.

Bioni aponta que a ideia de criar dispositivos que atravessassem diferentes setores foi tema já discutido por volta de 1970/80, ganhado força nos anos 2000, com a pressão internacional nos fóruns onde o Brasil participava, como o Mercosul. Embora nunca se tenha concretizado a ideia de uma regulação de proteção de dados para todos os países integrantes do Mercosul, os debates deflagrados por essa proposta serviram de combustível para a internalização do tema pelo poder executivo brasileiro (2021, p. 21).

Este processo intensificou os esforços para desenvolver os pontos-chave do texto para abordar não apenas questões limitadas ao campo nacional, além de exigir a inclusão de temas que antes não eram discutidos pelas antigas leis que tratavam do tema. Isso se deu em parte devido à projeção que o Regulamento Geral sobre a Proteção de Dados teve na Europa e no mundo, no período de 2012 a 2016, e que influenciou na criação e nos principais pontos fundantes da LGPD.

A iniciativa do Ministério da Justiça, em 2015, foi importante para a democratização e a participação política da toda a sociedade brasileira e de diversos setores e de organizações internacionais e grupos de pesquisa na construção da lei, a qual ocorreu sob a forma de duas consultas públicas, e que segundo Bioni:

---

[19] VALADARES, Pablo. A Comissão de Defesa do Consumidor da Câmara dos Deputados aprovou proposta que insere expressamente, no Código de Defesa do Consumidor, a informação de que a Lei Geral de Proteção de Dados Pessoais (LGPD) se aplica às informações existentes sobre o consumidor em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele. [...] A medida está prevista no substitutivo apresentado pelo deputado Jorge Braz (Republicanos-RJ) ao Projeto de Lei 786/19, da deputada Flordelis (PSD-RJ). Originalmente, a proposta proíbe o vendedor de armazenar em banco de dados físico ou eletrônico, sem autorização do consumidor, informações sobre cartão de crédito e débito ou outro instrumento de pagamento. **Agência Câmara de Notícias**. 2021. Acesso em 1 de out. de 2021. Disponível em: <https://www.camara.leg.br/noticias/791306-comissao-aprova-mencao-expressa-de-protecao-de-dados-no-codigo-de-defesa-do-consumidor/>.
Apesar das implicações sobre a dificuldade em aplicar a lei em casos de armazenamento de dados, a LGPD ganha maior destaque e validade quando relacionada com o conteúdo da Lei nº 8078/90, porque garante a vigência da proteção de dados em mais de um instrumento jurídico, e que é garantida exposição em todos os estabelecimentos comerciais, ampliando seu conhecimento pelos prestadores de serviço, mesmo que a lei ainda esteja em caráter conclusivo.

[20] Teve alteração pela Lei Complementar nº 166/2019.

> Recebeu mais de 1800 (mil e oitocentas) contribuições, de três tipos: i) comentários em cada parte do texto (artigos, incisos, parágrafos e alíneas); ii) comentários divididos por eixos temáticos; e iii) contribuições documentais em formato pdf. Além disso, o sistema permitia a participação de pessoas físicas e jurídicas. (2021, p. 24)

As empresas e agentes privados passaram a buscar nessa discussão formas de atenuar as sanções referentes ao controle dos dados, pois, no início do século XXI as informações se tornaram propriedade *res nullius* a partir do momento em que circulam pela rede.

Na outra ponta, a sociedade civil e as organizações internacionais defendiam a necessidade da legislação brasileira de revigorar o direito de propriedade e de privacidade, em vista do descontrole sobre os dados.

Busca-se nesta investida uma fórmula viável para o controle racional das informações, atentando à impossibilidade das agências brasileiras de segurança de atuar em todos os casos de cibercrimes. O que se almeja, nesse sentido, é a consolidação do resguardo das leis na internet e a preservação das informações.

A segunda consulta pública sobre a LGPD derivou na versão final enviada para a Câmara dos Deputados somente em 2016, o que fortaleceu o consenso entre as partes responsáveis pela criação da lei no legislativo. Esse projeto visava alcançar um acordo mais desenvolvido e multifacetado por meio do Projeto de Lei n.º 5.276, de 2016, que dispunha sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural, antes abarcado pelos projetos de lei nº 4060/2012[21] e o nº 330/2015.

Para o sucesso da aprovação da LGPD, foi necessário que houvesse o engajamento coletivo das diferentes frentes políticas e a convergência entre elas. Bruno classifica quatro pontos que propiciaram o acordo para a aprovação da lei:

> i) o escândalo Cambridge Analytica, que precipitou um debate por vezes restrito a círculos específicos para a grande mídia e o grande público; ii) a entrada em vigor, em maio de 2018, do Regulamento Geral de Proteção de Dados - RGPD europeu, que acirrou a necessidade de maior segurança jurídica quanto ao tratamento de dados no Brasil; iii) o desejo expresso do Brasil ingressar na Organização para a Cooperação e Desenvolvimento Econômico - OCDE, que exige, como boa prática, a regulamentação de uso de dados pessoais, assim como um órgão supervisor independente e autônomo; e, por fim, iv) uma articulação interna à Câmara dos

[21] Além do engajamento na criação de leis que abordassem a segurança de dados digitais e privacidade, foi criado também grupos de estudo especializados na temática cibernética, além da Comissão Especial da Câmara sobre Tratamento e Proteção de Dados Pessoais, que vigorou em 2016, através de audiências públicas a fim de aumentar o engajamento de especialistas e da sociedade no debate sobre a temática, ampliando o conhecimento e difundindo a informação através dos eixos públicos e a participação do setor privado e de ONGs, viabilizando a busca no consenso entre as partes, tendo em vista o multissetorialismo de ideias sobre o texto da LGPD.
Disponível em: <https://cd.jusbrasil.com.br/noticias/414897048/comissao-especial-debate-protecao-a-dados-pessoais>. Acesso em: 10 de out. de 2021.

> Deputados para a aprovação das alterações na Lei do Cadastro Positivo, que envolvia a aprovação da Lei Geral de Proteção de Dados como condição indispensável. (2021, p. 32)

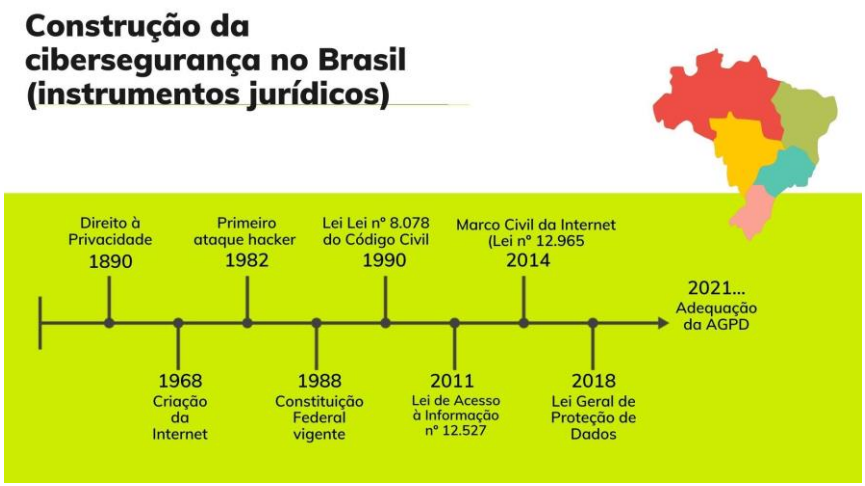
Tendo sido estes aspectos discutidos e acordados em um último debate, levantaram-se todas as ponderações e discussões conflitantes entre as partes para se chegar a um denominador comum em um processo *step by step*, com a avaliação dos pontos de forma transparente para todas as partes interessadas. O êxito desse processo facilitou a aprovação, sem a necessidade de cumprir o rito procedimental e tradicional do Congresso Nacional, e que gerou pouca discussão após sua validação.

A promulgação da Lei nº 13.709 3.709 de 14 de agosto de 2018[22] teve repercussão nacional e internacional devido à seu caráter inovador como ferramenta jurídica, pois o ambiente digital até os dias atuais é escasso de alternativas que tratem especificamente de crimes cibernéticos. Isso por se tratar ora de uma dimensão relativamente nova no direito brasileiro e internacional, que tende a se manter resguardada sob amparo da CF e das demais ramificações do direito existente, pelo fato de que um invasor pode acessar os dados de indivíduos e empresas de qualquer lugar, sem ou com difícil identificação e em quantidade massiva.

É fato que o direito subjetivo resguarda que uma pessoa seja a titular de suas informações, e sobre elas, tenha total poder, podendo cancelar qualquer acordo que lhe prejudique, como ampara o Direito de Arrependimento, disposto pelo Artigo nº 49 do Código do Consumidor Brasileiro, Lei 8.078/90 para contratos. Além disso, não se estipula um prazo específico para a quebra de um contrato em caso de cláusulas abusivas ou ilícitas baseadas em dolo, coação ou de erro caracterizado de acordo com o Código Civil.

[22] SENADO. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 01 de set. de 2021.

Tabela 2: Construção da cibersegurança no Brasil: (instrumentos jurídicos)



Fonte: BRAGA, Noelson, 2021.

Com o desenvolvimento do Direito junto aos padrões das relações no ambiente digital, a elaboração da Lei Geral de Proteção de Dados em 2018, representou um avanço significativo na regulação dos dados como nunca visto antes na história brasileira. Talvez a necessidade jurídica fosse um pilar fundamental para a organização das estruturas sociais e comerciais, pois é nela que é garantido o poder de coerção e da administração da atividade cibernética. Sua fundamentação surgiu pela demanda nacional em controlar a atividade no país, de forma a regularizar alguns serviços e coibir outros.

Segundo Bioni, a LGPD se caracteriza por um processo multiparticipativo e particularmente bem-sucedido na produção de "consensos pragmáticos" (p. 16-17, 2021). Isso significa que os esforços estatais e da sociedade civil foram efetivados conjuntamente em um dispositivo, que começaria a valer em 2020, mas que ainda busca se adequar às limitações e aos eixos onde deve atuar.

Em relação a visibilidade internacional do Brasil na proteção digital, no ano de 2021 foi registrada a subida brasileira no ranking de cibersegurança da ONU. Esta mudança foi da 71ª posição para o 18º lugar numa lista com 193 países[23], provando que este processo, que levou 15 anos, tem finalmente demonstrado resultados satisfatórios, mesmo em um país de política cibernética fechada. Não obstante, a nova pontuação não desmistifica a necessidade do país em ampliar o escopo técnico para combater as novas ameaças.[24]

[23] BONIN, Robson. Brasil sobe 53 posições em ranking de cibersegurança da ONU: Apesar de ataques recentes, país saiu da posição 71 para a 18. Disponível em: <**https://veja.abril.com.br/blog/radar/brasil-sobe-53-posicoes-em-ranking-de-ciberseguranca-da-onu**/>. Acesso em 07 nov. 2021.
[24] Agência Senado. Brasil é 2º no mundo em perdas por ataques cibernéticos, aponta audiência. 2019.

4 RGPD e LGPD: comparativos e projeções

A legislação brasileira acerca da cibersegurança se espelha nos pontos principais do Regulamento Geral sobre a Proteção de Dados da UE, a qual introduziu avanços nas relações do ciberespaço ampliando o campo de jurisdição dos países em seus territórios. Apesar da inspiração que a LGPD possa ter tido no regulamento europeu, observa-se que a mesma também toma em conta o histórico de casos e tentativas nacionais em combater os ciberataques, mesmo que indiretamente.

Por um lado, o Regulamento - UE 2016/679 prevê o amparo para as pessoas, empresas ou organizações da União Europeia, enquanto a lei brasileira limita o seu texto somente às suas delimitações territoriais, sem projetar soluções com países vizinhos. Apesar disso, o RGPD demonstra ser mais robusto em seu escopo e também na dimensão técnica, além de contemplar a cooperação internacional, que é necessária ao combate aos ciberataques.

O conteúdo do Regulamento e da Lei Geral de Proteção de Dados designa o público alvo e os limites da lei para as atividades profissionais, comerciais, e as da esfera pessoal e doméstica, somente em casos do exercício de atividades socioculturais ou financeiras. Essa definição tem por objetivo otimizar os esforços dos Estados-membro em garantir a eficiência das leis, cabendo aos usuários o papel de responsável sobre seus próprios dados e também de responsável por onde distribui seus dados.

No Brasil, o papel da Autoridade Geral de Proteção de Dados visa a cooperação com a sociedade no que tange o comprometimento da população brasileira em somente solicitar o apoio da instituição nas denúncias que lhes forem competentes, a fim de evitar a sua sobrecarga e otimizar a qualidade de investigação e autuação. Observando a teoria realista, o Brasil definiu sua defesa a partir do pensamento voltado no *self-help*, enquanto a União Europeia ampliou a integração regional, mesmo que para suprir suas necessidades e garantir vantagens no jogo de poder.

Medindo esforços para que o regulamento europeu tenha êxito, o Conselho e o Parlamento especificam os principais temas aos quais os países e agências devem atentar para o combate do ciberterrorismo, são eles: 1-aumentar a ciber-resiliência; 2-combater a cibercriminalidade; 3-fomentar a ciberdiplomacia; 4-reforçar a ciberdefesa; 5-impulsionar a

investigação e a inovação e 6-proteger infraestruturas críticas. (Conselho da União Europeia, 2021).

No Brasil percebe-se a semelhança quanto ao texto nos pontos referentes aos objetivos da lei. Em comparação ao Regulamento UE, o artigo nº 4º da LGPD também limita que esta lei não se aplica ao tratamento de dados pessoais:

> Esta Lei não se aplica ao tratamento de dados pessoais: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei. (BRASIL, 2019)

Os europeus desenvolveram diversos mecanismos de combate aos ciberataques referentes a transportes, a energia, a saúde e às finanças por conta da associada relação cada vez mais presente com a tecnologia digital, e contemplou também alternativas que promovessem o desenvolvimento em tais campos em tempos de pandemia. Articulou, assim, a economia ao bem-estar social de sua população, que não está imune aos ciberataques.

Sobre as ponderações de teor econômico e suas novas ferramentas digitais, o Brasil não definiu um sistema específico para controle da atividade financeira de investimentos e das criptomoedas. Essas questões regulatórias relacionadas aos bancos digitais e físicos permanecem sob competência do Banco Central. Em matéria dos criptoativos como dados como propriedade, inexiste internacionalmente legislação para a herança digital[25] por não haver intermediação de instituições bancárias públicas e privadas ou por bancos centrais, sendo este assunto para discussão, em vista da perspectiva do do papel cada vez mais relevante das criptomoedas no futuro das relações comerciais bancárias num prisma geral, e que é de teor cibernético.[26] Por outro lado, a UE prevê novas regras para combater a fraude em pagamentos que não em numerário, com previsão de vigência para ainda em 2021.

---

[25] As principais moedas digitais no mercado tecnológico são: Bitcoins, Ethereum, Binance Coin, Bitcoin Cash, Litecoin e Ripple. ISMAR, Bruno, 2021. Disponível em: _____ <https://renovainvest.com.br/blog/lista-de-criptomoedas-conheca-10-das-principais-moedas-digitais-do-mundo/#:~:text=O%20bitcoin%20%C3%A9%20a%20moeda,sistema%20de%20pagamentos%20global%20descentralizado.&text=O%20bitcoin%20%C3%A9%20minerado%20e,sistema%20computacional%20complexo%20chamado%20blockchain.>. Acesso em 20 abr. 2021.

[26] A transação das criptomoedas é registrada em rede de internet através de um sistema de computadores integrado conhecido como *point to point* (P2P), que garante que estes dados não sejam violados. Além disso, no universo do dinheiro digital, para garantir que a informação sobre o valor da carteira de cada indivíduo e suas transações sejam registradas, são armazenados tais registros sob o sistema de *blockchain.* Ver: GREGORY, Gabriel. Herança de criptoativos – Como funcionaria? **JUSBRASIL**, 2020. Disponível em: _____

Em ambos os contextos é caracterizado o compromisso em promover confiança, na UE entre os países e suas populações, e no Brasil um consenso nacional restrito ao seu território, o que não possibilita também as trocas comerciais entre países, visto que o Brasil detém da lei exclusivamente para o uso doméstico, sem a participação de outros países vizinhos.

A União Europeia moderniza as relações entre seus membros mediante esforço coletivo na inovação tecnológica de criptografia, da diplomacia e o desenvolvimento das ferramentas e de um substrato institucional contra o ciberterrorismo e os ciberataques. Além disso, há também amparo das instituições competentes na criação de regras, requisitos e normas coletivas, enquanto no Brasil, tem-se um histórico de projeção do sucesso da Lei nº 13.709/2018 através do consenso multisetorial que deu margem à sua criação e aprovação. Este processo atende às demandas de diversos grupos, mesmo que possa haver impasses futuros.

Do lado brasileiro foi criada a Autoridade Nacional de Proteção de Dados - AGPD, que apesar de recente, responsabiliza-se sobre as investigações e autuação dos casos em que a LGPD autoriza, e do lado europeu há a Agência da UE para a Cibersegurança, que sucede a antiga Agência Europeia para a Segurança das Redes e da Informação - ENISA.

A nova Agência da UE para a Cibersegurança baseia-se nas estruturas da sua antecessora, a Agência Europeia para a Segurança das Redes e da Informação - ENISA, de mesma sigla, reforçando a luta no ambiente digital e garantindo a vigência da lei sobre o ciberespaço.

Outra agência europeia que atua em cibersegurança é o Centro Europeu da Cibercriminalidade (Europol), tratando de roubo de dados, invasão da propriedade intelectual, exploração sexual infantil na "*darkweb"* e na *surface web,* tema este que como visto, é objeto de normativa internacional para a prevenção e detecção de possíveis ameaças a este público*"*, entre outros assuntos.

É notável o desempenho e progresso destas instituições na busca por aperfeiçoamento dos profissionais e das ferramentas para inibir o avanço dos cibercrimes. Tratando de uma perspectiva internacional, a Plataforma Multidisciplinar Europeia contra as Ameaças Criminosas - EMPACT recebe o mérito pelo avanço na missão conjunta para identificar, priorizar e combater as ameaças representadas pela criminalidade internacional organizada.

Impactada pela necessidade da ação rápida, mas com certa dificuldade em alcançar êxito, as autoridades de proteção de dados ampliam as tecnologias de rastreio e descriptografia

<https://ggregory096.jusbrasil.com.br/artigos/786630733/heranca-de-criptoativos-como-funcionaria>. Acesso em 20 abr. 2021.

de mensagens e informações acerca de criminosos e suas provas, a fim de ampliar o amparo legal para a aplicação de sanções penais, tanto no Brasil[27] quanto na Europa. O que difere os dois casos é o empenho cooperativo dos países da UE em elaborar novas regras que tornarão o acesso transfronteiras a provas eletrônicas mais fácil e mais rápido, visando negociação também com os EUA. (Conselho da União Europeia, 2021).

5 CONSIDERAÇÕES FINAIS

Um dos maiores problemas que a cibersegurança apresenta no Brasil talvez seja a desinformação desenfreada e o *accountability* na questão da autuação de sanções nos casos de desobediência da legislação brasileira. O espaço cibernético cresce todos os dias. Os aparatos técnicos e científicos de controle, apesar de se esforçarem na resiliência, demonstram atraso significativo na tratativa da proteção de dados e do resguardo real do direito à privacidade dos usuários na rede.

Projetando um cenário favorável aos avanços de uma agenda efetiva de proteção cibernética, a União Europeia por meio do Conselho Europeu, do Parlamento Europeu e suas demais instituições tendem a alcançar resultados mais satisfatórios que o Brasil, observando os esforços dedicados, o potencial dos países no quesito informação e preparação técnica e tecnológica, e principalmente na diplomacia através da cooperação internacional, pois nesta rede conectada, as informações perpassa os limites fronteiriços destes Estados pela busca do bem-comum.

No caso brasileiro não se avalia aqui uma situação tão díspar, mas a construção da lei unicamente nacional, mesmo que com o fomento das ideias multissetoriais ainda necessita do amparo dos países vizinhos, pois no caso europeu apresentou resultados positivos e ampliou a confiança do grupo em questões estratégicas e comerciais.

Deve-se perceber que o motivo que levou o Brasil à decisão de não incluir outros países do Cone Sul ou do próprio Mercosul em sua agenda de cibersegurança está relacionada com a política nacional que o país adota em seus segmentos de segurança, e pela ideia perpetuada de anarquia internacional que os realistas abordavam desde o início dos estudos de Relações Internacionais.

Na construção realista em que esta pesquisa se baseou, e avaliando o segmento da política internacional para a temática trabalhada, há inclinação para os países buscarem

[27] Devido a recente instauração da ANPD, os conteúdos referentes a crimes cibernéticos mais desenvolvidos se concentravam nas delegacias especiais de repressão aos crimes cibernéticos e aos demais órgãos especializados.

cooperação com seus adversários no combate das novas ameaças, de forma isolada e visando objetivos em que há resultados de ganha-ganha, como no novo acordo entre os Estados Unidos e a Rússia em combater a iminente ameaça digital que vigora. O Brasil se espelhará nas ações norte-americanas, se permanecer com o espelhamento estratégico, e a União Europeia permanecerá com o empenho na busca pelo aperfeiçoamento do aparato técnico e tecnológico que vem desenvolvendo, com o intuito de fomentar o desenvolvimento na região e fortalecer a defesa dos países membros.

Cabe a estas agendas e instituições ampliar o debate público acerca da proteção de dados para temas mais profundos e pouco discutidos nos fóruns de segurança digital, como a projeção do direito acerca dos dados como propriedade em uma esfera econômica e política. São exemplos das novas temáticas a serem abarcadas neste debate, como a herança de criptomoedas e o respeito aos dados *post mortem*, além de outros temas como a ampliação do reconhecimento facial na defesa x progressão do uso indevido da imagem, descrição algorítmica, entre outros.

A diplomacia digital é, de fato, uma das armas mais eficazes no desenvolvimento de novas alternativas para o controle da atividade cibernética no Brasil, Europa e no mundo, pois com as diversas novas ameaças, cabe inovação e cooperar para o fomento de soluções e respostas rápidas às atuais ameaças e à necessidade de maior ordem na internet.

A projeção para o Brasil no segundo semestre de 2021 é do aumento no orçamento para a defesa cibernética, e mesmo que para muitas autoridades políticas e empresas o tema seja visto como gasto, as exigências da nova lei tornam mais eficaz a imposição indireta da melhoria dos dispositivos de segurança de dados.[28]

Enquanto isso, na Europa, os países da UE dedicam atenção especial ao assunto, ocupando 18 dos 20 lugares cimeiros do Índice Mundial de Cibersegurança - *GCI*, e promovendo o desenvolvimento econômico e social por meio do conhecimento da cibersegurança, com projeção de crescimento de 17 % ao ano.

Percebe-se aqui que a cibersegurança se torna, no século XXI, tema de grande relevância e repercussão devido não somente à maior inclusão digital nos últimos anos, mas também pela relação direta das novas tecnologias com os setores principais das sociedades contemporâneas voltados para o desenvolvimento, lazer e econômico.

---

[28]LUCENA, André. Crescimento nos investimentos em cibersegurança e o que esperar para o segundo semestre. Olhar Digital. 2021. Disponível em: <https://olhardigital.com.br/2021/08/31/colunistas/crescimento-nos-investimentos-em-ciberseguranca-e-o-que-esperar-para-o-segundo-semestre/>. Acesso em 20 out. 2021.

As leis discutidas nesta pesquisa demonstram que há limites técnicos e humanos para que haja um sistema consideravelmente aceitável de defesa cibernética, mas a sociedade civil deve, junto às empresas e instituições governamentais, garantir a cooperação no combate a desinformação e às *fake news* e nos cuidados básicos para a preservação dos dados na internet, garantindo o uso responsável e satisfatórios para as partes, a fim de não esgotar as energias das agências com um número abusivo de denúncias.

Por fim, os dados apresentados demonstram que o empenho europeu tem se mostrado eficaz não apenas no combate aos cibercrimes, mas também na união dos países em construir uma Europa mais conectada e desenvolvida, com o apoio da tecnologia e conhecimento compartilhado, mas tendem a colapsar os interesses dos países se não houver um canário vantajoso para a cooperação. O Brasil segue a passos largos de alcançar êxito na cibersegurança, mas tem avançado pouco a pouco, conforme o país tem investido em leis específicas para tratamento do tema em escala nacional.

Ambos os países têm o objetivo de se aperfeiçoar para combater as novas ameaças e resguardar o direito à privacidade por meio do preparo dos sistemas de segurança tecnológica e com a especialização de agentes. Contudo, estes desafios necessitam tempo e flexibilização política à cooperação e à diplomacia, desafios que dialogam com a natureza dos estados, se percebidos sob uma roupagem realista de Relações Internacionais.

REFERÊNCIAS BIBLIOGRÁFICAS

ACÁCIO, Igor; SOUZA, Gills. Segurança internacional no século XXI: o que as teorias de Relações Internacionais têm a falar sobre o ciberespaço? 36º Encontro Anual da Anpocs Política Internacional – GT28, 2012.

ÂMBITO JURÍDICO. **Considerações sobre bens na Teoria Geral do Direito Civil**. Disponível em: <https://ambitojuridico.com.br/cadernos/direito-civil/consideracoes-sobre-bens-na-teoria-geral-do-direito-civil/>. 2006. Acesso em 19 abr. 2021.

BIONI, Bruno. Proteção de dados: Contexto, narrativas e elementos fundantes. Sociedade Individual de Advocacia, São Paulo, 2021, 425 p.. Disponível em: <https://d335luupugsy2.cloudfront.net/cms%2Ffiles%2F108127%2F1629122366livro-LGPD-Bruno-Bioni-completo-internet-v2.pdf> ISBN 978-65-995360-0-7

BLOOMBERG. Na era do bitcoin, o velho problema das heranças. OGLOBO, 2018. <Disponível em: https://oglobo.globo.com/economia/na-era-do-bitcoin-velho-problema-das-herancas-22395921>. Acesso em 19 abr. 2021.

BOSE, Nandita. "EUA e UE vão discutir regulação conjunta de gigantes de tecnologia em encontro". CNN Brasil. 2021. Disponível em: <https://www.telesintese.com.br/comissaria-da-

ue-defende-regulacao-de-competicao-mais-abrangente-para-big-techs/>. Acesso em 11 nov. 2021.

CARDOSO, Oscar. Glossário da Lei Geral de Proteção de Dados. 2020. Administradores. Disponível em: <https://administradores.com.br/artigos/gloss%C3%A1rio-da-lei-geral-de-prote%C3%A7%C3%A3o-de-dados-4>. Acesso em: 19 abr. 2021.

Comissão Europeia. Cibersegurança: como combate a UE as ciberameaças. Disponível em: <https://www.consilium.europa.eu/pt/policies/cybersecurity/>. Acesso em 03 ago. 2021.

Comissão Europeia. Cronologia – cibersegurança. Disponível em: <https://www.consilium.europa.eu/pt/policies/cybersecurity/timeline-cybersecurity/>. Acesso em 03 ago. 2021.

Comissão Europeia. Sobre o regulamento e a proteção de dados. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_pt>. Acesso em 03 ago. 2021.

JÚNIOR, Dimas Pereira Duarte. Accountability e Relações Internacionais. Ponto & Vírgula, n. 4, 2008. Disponível em: <https://revistas.pucsp.br/index.php/pontoevirgula/article/view/14152>. Acesso em 08 out. 2021. DOI <https://doi.org/10.23925/1982-4807.2008i4p%25p>.

FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Antonio. A Construção Multissetorial da LGPD: História e Aprendizados, in: A Lei Geral de Proteção de Dados Pessoais: Lgpd. Editora Revista dos Tribunais. *ed.* 2021, 2021.

G1 Economia. Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber.. 2021. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml>. Acesso em 13 mar. 2021.

GOMES, Waldo. Qual é o impacto da LGPD no vazamento de dados? **Mobile Time**. 2020. Disponível em: https://www.mobiletime.com.br/artigos/29/07/2020/qual-e-o-impacto-da-lgpd-no-vazamento-de-dados/#:~:text=O%20vazamento%20de%20dados%20pessoais,quanto%20para%20os%20j%C3%A1%20clientes.&text=Bloqueio%20e%20elimina%C3%A7%C3%A3o%20dos%20dados,50%20milh%C3%B5es%20por%20cada%20infra%C3%A7%C3%A3o. Acesso em 13 mar. 2021.

GREGORY, Gabriel. Herança de criptoativos – Como funcionaria?. JusBrasil, 2020. Disponível em: <https://ggregory096.jusbrasil.com.br/artigos/786630733/heranca-de-criptoativos-como-funcionaria>. Acesso em 20 abr. 2021.

GUIALGPD. LGPD Comentada.. Disponível em: <https://guialgpd.com.br/lgpd-comentada/> Acesso em 14 mar. 2021.

HURIEL, Louise Marie. Brazil's First National Cybersecurity Strategy: An Analysis of its Past, Present and Future. GeorgiaTech, 2020. Disponível em:

<https://www.internetgovernance.org/2020/04/05/brazils-first-national-cybersecurity-strategy-an-analysis-of-its-past-present-and-future/>. Acesso em 01 nov. 2021.

JUSBRASIL. **O direito de arrependimento do consumidor.** Antunes Advocacia. Disponível em: <https://antunes-advocacia.jusbrasil.com.br/noticias/2994570/o-direito-de-arrependimento-do-consumidor#:~:text=O%20consumidor%20pode%20desistir%20do,Par%C3%A1grafo%20%C3%BAnico.> Acesso em 13 mar. 2021.

KELLO, Lucas. *The Virtual Weapon and International Order*. Yale University Press, 2017, 336 p. ISBN 0300220235.

KHANNA, Tarun. *Trust: Creating the Foundation for Entrepreneurship in Developing* Countries. Berrett-Koehler Publishers, 2018.

LANDIM, Emiliano. Bens digitais: O novo tipo de herança que surgiu na internet. AURUM. 2018. Disponível em: <https://www.aurum.com.br/blog/o-que-sao-bens-digitais/>. Acesso em 20 abr. 2021.
LIMA, Paulo *et al*. Marx como referencial para análise de relações entre ciência, tecnologia e sociedade. Ciência & Educação (Bauru) [online]. 2014, v. 20, n. 1. Acesso em 15 out 2021, pp. 175-194. Disponível em: <https://doi.org/10.1590/1516-731320140010011>. Epub 02 Abr 2014. ISSN 1980-850X. https://doi.org/10.1590/1516-731320140010011.

LOURENÇO, Gabriel D. Killware: invasões de computadores que matam fisicamente soam alerta para autoridades. **Olhar Digital**. 2021. Disponível em: <https://olhardigital.com.br/2021/10/15/seguranca/killware-ameaca-virtual-matar-a-distancia/>. Acesso em: 15 out. 2021.

Metrópoles. MPDFT investiga mais uma empresa por venda de dados pessoais. 2020. Disponível em: <https://www.metropoles.com/distrito-federal/mpdft-investiga-mais-uma-empresa-por-venda-de-dados-pessoais>. Acesso em 19 mar. 2021.

PODER360. Brasil tem 2 dispositivos digitais por habitante, diz FGV. 2021. Disponível em: <https://www.poder360.com.br/tecnologia/brasil-tem-2-dispositivos-digitais-por-habitante-diz-fgv/>. Acesso em 10 jul 2021.

RIBEIRO. Letícia. Bens. DIREITONET. Disponível em: <https://www.direitonet.com.br/artigos/exibir/2631/Bens#:~:text=Bens%20s%C3%A3o%20valores%20materiais%20ou,de%20uma%20rela%C3%A7%C3%A3o%20de%20direito.&text=S%C3%A3o%20bens%20jur%C3%ADdicos%20os%20de,um%20livro%2C%20ou%20um%20CD.>. Acesso em 20 abr. 2021.

RIELLI, Mariana. Proteção de dados: contexto, narrativa e elementos fundantes: *Uma resenha do livro de Bruno Bioni, fundador do Data Privacy Brasil*. **Coluna JOTA. 2021.** Disponível em:<https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/protecao-de-dados-contexto-narrativa-e-elementos-fundantes-27082021>. Acesso em 01 set. 2021.

SENADO. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 01 jul. 2021.

SILVA, Bruna. Reflexões sobre a herança digital e o bitcoin. 2020. **CONSULTOR JURÍDICO**. Disponível em: <https://www.conjur.com.br/2020-mai-24/bruna-lauviah-reflexoes-heranca-digital>. Acesso em 20 abr. 2021.

TV SENADO. "Constituição brasileira é de país de primeiro mundo", diz Ayres Britto. 2018. Disponível em: <https://www12.senado.leg.br/noticias/materias/2018/08/02/constituicao-brasileira-e-de-pais-de-primeiro-mundo-diz-ayres-britto>. Acesso em 10 mar. 2021.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. 27 de abril de 2016. *Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Acesso em 12 jul 2021.

VARELLA, Thiago. FaceApp rouba os meus dados? Veja 6 coisas que você devia saber sobre ele. **UOL Segurança.** 2020. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/06/15/faceapp-rouba-os-meus-dados-seis-coisas-que-voce-devia-saber-sobre-ele.htm#:~:text=O%20FaceApp%2C%20aplicativo%20que%20usa,ficar%20na%20moda%20no%20Brasil.&text=O%20app%20%C3%A9%20acusado%20de,de%20sua%20pol%C3%ADtica%20de%20privacidade.>. Acesso em 13 mar. 2021.

WILLES J. *The Right to Privacy.* In Millar v. Taylor, 4 Burr, 1890. p.2303-2312.