III. Introdução

O objetivo principal deste estudo é analisar ocorrências de crimes cibernéticos que afetam os usuários de redes digitais, caracterizando aqueles que usufruem como forma de lazer, para trabalho ou estudo, bem como investigar as consequências legais para quem cometa tais crimes e se aproveite das lacunas existentes na era moderna, caracterizada pelo vasto uso da internet.

Além disso, a proteção dos direitos fundamentais, como a privacidade e a liberdade de expressão, deve ser cuidadosamente considerada no desenvolvimento de políticas e leis relacionadas aos cibercrimes. O equilíbrio entre segurança e liberdade é crucial para garantir que as medidas de combate ao crime não resultem em violações dos direitos dos cidadãos.

O resumo adota o método hipotético-dedutivo para maximizar os resultados da pesquisa científica. Isto é feito ao formular hipóteses, deduzir suas implicações e realizar testes empíricos para verificar se essas implicações estão alinhadas com a realidade e alinhadas com o contexto atual, que é regulado pelas leis penais e processuais.

IV. Desenvolvimento

No cenário atual, a crescente digitalização das atividades humanas tem gerado novos desafios para o Direito Penal, particularmente no combate aos cibercrimes. Com base no método hipotético-dedutivo, esta pesquisa parte da hipótese de que o arcabouço jurídico penal tradicional é insuficiente para lidar com eficácia com os desafios dos crimes cibernéticos. A fim de testar essa hipótese, serão analisados diversos aspectos dos cibercrimes, incluindo a jurisdição transnacional, a proteção de dados, a identificação de criminosos digitais e a adaptação das leis penais.

As legislações penais vigentes são inadequadas para enfrentar a complexidade dos cibercrimes. No entanto, em 27 de maio de 2021 foi sancionada a Lei 14.155 que altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato.

A digitalização das interações humanas e do cibercrime tornou a proteção dos dados pessoais um aspecto importante do direito penal e digital. A Lei LGPD do Brasil, promulgado pela Lei nº 13.709/2018, é um importante marco regulatório para proteger a privacidade e a segurança da informação. O estudo é hipotético e parte do pressuposto de que a LGPD é um fator-chave na prevenção e redução do crime cibernético, fornecendo uma base sólida para a proteção de dados pessoais e a promoção da segurança digital.

A LGPD estabelece padrões rígidos para o tratamento de informações pessoais, assim como a Lei 12.737/2012, também conhecida como Lei Carolina Dieckmann, que inseriu no código penal o crime de invasão de dispositivo informático, isto é, celulares, notebooks, tablets e etc. A primeira lei a punir crimes cibernéticos dispõe sobre a invasão de dispositivos informáticos alheios, e tem como intuito obter, adulterar ou destruir dados ou informações sem prévia autorização. E assim em conjunto essas Leis exigem que os setores público e privado cumpram com suas responsabilidades. A hipótese principal é que a implementação efetiva das Leis pode reduzir significativamente a ocorrência de crimes cibernéticos, como roubo de identidade, fraude financeira, violação de privacidade, etc.

A transformação digital em todas as áreas econômicas foi acelerada pela pandemia do COVID-19. Por outro lado, os novos tempos tornaram os usuários mais vulneráveis a ataques cibernéticos, o que aumentou a demanda por apólices de seguro que os protejam contra esse tipo de ameaça. Os números de tentativas de crime cibernético são significativos no geral e justificam a intensa mobilização das seguradoras para encontrar soluções que assegurem dados pessoais da população e assuntos sigilosos do Estado.

O Brasil é o segundo país mais afetado por ataques cibernéticos na América Latina e Caribe, com 103,1 bilhões de tentativas, um aumento de 16% em relação aos registrados em 2021. No México, foram 187 bilhões de tentativas em 2022. “Os números explicam a razão de o tema cyber segurança estar na pauta de todos os agentes do setor e precisa ser enfrentado com urgência. O cenário dos riscos cibernéticos evoluiu rapidamente por conta da digitalização dos processos e foi agravado pela pandemia”, comentou o diretor técnico da Confederação Nacional das Seguradoras (CNseg), Alexandre Leal.

V. Conclusão

É evidente que ainda há grandes obstáculos a serem vencidos. A legislação e os regulamentos precisam ser aprimorados devido à rápida evolução da tecnologia e às mudanças nas práticas de proteção e asseguramento de dados. Além disso, a salvaguarda de dados pessoais envolve uma questão global que requer a colaboração entre várias jurisdições e a aplicação de padrões internacionais.

O direito penal, historicamente focado em crimes físicos e tangíveis, enfrenta o desafio de se modernizar para abarcar as complexidades dos delitos virtuais. Isso inclui a necessidade de definir claramente o que constitui um cibercrime, de estabelecer jurisdições adequadas para processar esses crimes e de criar penas proporcionais às novas modalidades de infração. Além disso, a cooperação internacional torna-se essencial, visto que a natureza sem fronteiras da internet permite que criminosos operem de qualquer lugar do mundo, atingindo vítimas em múltiplas jurisdições.

É justo que governos, empresas e pessoas em geral colaborem para garantir um tratamento ético e responsável dos dados confidenciais, para proteger os direitos individuais e a privacidade na era da informação. O investimento na área da segurança digital deve-se ser levado a sério e estabelecida dentre os principais pilares do Estado,

como a Coordenadoria Estadual de Combate aos Crimes Cibernéticos (COECIBER), o primeiro órgão especializado no combate aos crimes digitais do Ministério Público brasileiro, criada pioneiramente em 16 de junho 2008, órgãos construtivos que visam tutelar e aplicar sentenças penais cada vez mais rígidas e eficazes contra criminosos que atuam nesta área.

Resumidamente, lidar com os crimes cibernéticos no campo do direito penal demanda uma estratégia versátil que integre novas leis, colaboração global, preservação dos direitos básicos e a promoção de avanços tecnológicos e educacionais. Unicamente por meio desse enfoque abrangente será viável reduzir os perigos ligados à cibercriminalidade e garantir que a sociedade desfrute dos benefícios da era digital de maneira segura e resguardada.

VI. Referências preliminares

SIMAS, Diana Viveiros de. O cibercrime. 2014. 168f. Dissertação (Mestrado em Ciências JurídicoForenses). Universidade Lusófona de Humanidades e Tecnologias. Lisboa. 2014.

SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. A convenção de Budapeste e a leis brasileiras. In: Anais do 1º Seminário "Cibercrime e Cooperação Penal Internacional". Org. CCJ-UFPB e Association Internacionale de Lutte Contra la Cybercriminalite (França), João Pessoa/PB, maio de 2009. Acesso em: http://www.egov.ufsc.br/portal/conteudo/conven%C3%A7%C3%A3o-de-budapeste-e-leis-brasileiras.

BRASIL, Lei Nº14.155 de 27 de maio de 2021 Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato.
SITE PARA LEVANTAMENTO DE DADOS ESTATÍSTICOS, https://www.infomoney.com.br/negocios/brasil-aparece-em-2o-em-ranking-de-ataques-ciberneticos-como-se-proteger/

BRASIL, Lei Nº13.709 de 14 de agosto de 2018, lei geral de proteção de dados pessoais (LGPD). (redação dada pela lei nº 13.853, de 2019). Vigência.

BRASIL, Lei Nº12.737 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. Vigência.