UNIVERSIDADE PRESBITERIANA MACKENZIE
FACULDADE DE DIREITO

GIOVANNA MONTEIRO MENDES

CIBERCRIMINALIDADE E NEGLIGÊNCIA DIGITAL:
AUTOCOLOCAÇÃO EM RISCO DA VÍTIMA

SÃO PAULO
2023

GIOVANNA MONTEIRO MENDES

CIBERCRIMINALIDADE E NEGLIGÊNCIA DIGITAL:
AUTOCOLOCAÇÃO EM RISCO DA VÍTIMA

Trabalho de Conclusão de Curso apresentado como requisito para obtenção do título de Bacharel no Curso de Direito da Universidade Presbiteriana Mackenzie.

Orientadora: Profª Dra. Thamara Duarte Cunha Medeiros

SÃO PAULO

2023

GIOVANNA MONTEIRO MENDES

CIBERCRIMINALIDADE E NEGLIGÊNCIA DIGITAL:
AUTOCOLOCAÇÃO EM RISCO DA VÍTIMA

Trabalho de Conclusão de Curso apresentado como requisito para obtenção do título de Bacharel no Curso de Direito da Universidade Presbiteriana Mackenzie.

Aprovada em ___/___/___

Banca Examinadora

Examinador:

Examinador:

Examinador:

DEDICATÓRIA

À minha família, meu bem maior, pela história de luta, coragem, perseverança e superação.
À minha mãe, Lucilene, por todo incentivo e por ter me ensinado o verdadeiro significado da palavra amor em sua amplitude. Dona de um caráter incontestável e de um coração descomunal, saiba que a senhora é a mulher mais incrível que eu já conheci.
Aos meus irmãos, Sergio, Vanessa e Ricardo, por todo carinho e confiança depositadas ao longo do tempo. Encontrei em cada um de vocês, amizade, cumplicidade, dedicação e inspiração.

AGRADECIMENTOS

À minha orientadora, Dra. Thamara Duarte Cunha Medeiros e aos meus mestres, pelos ensinamentos e pela atenção dispensada, ampliando assim nossas perspectivas, nos permitindo antever um futuro melhor. Toda minha admiração e respeito, incontestáveis exemplos de competência e dedicação.

À minha família, por todo apoio e incentivo em todos os meus sonhos e metas, sem vocês eu não conseguiria ter realizado nenhum deles. Quero destacar apenas o amor que há dentro de cada um deles, amor em forma de companheirismo e cuidado. Meu combustível diário de felicidade e motivação.

Aos meus amigos e a todos aqueles que contribuíram de alguma forma para que eu chegasse até aqui, tenham certeza de que dentro do meu coração está guardado um gesto, um olhar, uma palavra de incentivo e de carinho, que cada um de vocês me dirigiu quando precisei.

Feliz por finalizar esse ciclo.

Por fim, a todos, o meu muito obrigada.

CIBERCRIMINALIDADE E NEGLIGÊNCIA DIGITAL:
AUTOCOLOCAÇÃO EM RISCO DA VÍTIMA

GIOVANNA MONTEIRO MENDES

Resumo: O presente artigo trata da abordagem dos delitos praticados no ambiente cibernético e dos riscos e consequências para os usuários desinformados e negligentes. Tal análise concluirá que as condutas praticadas na nova realidade virtual apontam para a necessidade de adaptação dos usuários da rede, uma vez que a legislação vigente relacionada a presente temática é defasada, ou seja, não é suficiente e adequada a essa nova realidade e, não só isso, somente poderá ser eficiente na prática com uma vítima atenta e disposta à proteção. A postura do usuário no ciberespaço é muito significativa para a sua própria proteção nas redes, o melhor combate à cibercriminalidade hoje é a prevenção.

Palavras-chave: Cibercriminalidade. Autorisco. Vítima. Cibervitimização. Educação Digital.

CYBERCRIMINALITY AND DIGITAL NEGLIGENCE:
SELF-PLACEMENT AT THE RISK OF THE VICTIM

Abstract: This article deals with the approach to crimes committed in the cyber environment and the risks and consequences for uninformed and negligent users. This analysis will conclude that the conduct practiced in the new virtual reality points to the need for adaptation of network users, since the current legislation related to this topic is outdated, that is, it is not sufficient and adequate to this new reality and, not Tha alone can only be effective in practice with an attentive victim willing to protect. The user's stance in cyberspace is very significant for their own protection on networks, the best fight against cybercrime today is prevention.

Keywords: Cybercrime. Self-risk. Victim. Cyber victimization. Internet. Digital education.

Sumário: 1. Introdução. 2. Legislação Brasileira acerca dos Crimes Cibernéticos. 2.1. Lei Carolina Dieckmann – Lei n° 12.737/2012. 2.2. Marco Civil da Internet – Lei n° 12.765/2014. 2.3. Lei Geral de Proteção de Dados Pessoais – Lei n° 13.709/2018. 2.4. Convenção de Budapeste – Decreto n° 11.491/2023. 3. Características e Evolução dos Crimes Cibernéticos. 4. Vitimologia e Vitimodogmática. 5. Autocolocação em risco da vítima nas redes. 6. Riscos no Ciberespaço à luz da Negligência da Vítima Digital. 6.1. Consequências. 6.2. Educação Digital. 7. Considerações Finais. 8. Referências Bibliográficas.

1. INTRODUÇÃO

A princípio, é patente o avanço tecnológico que aconteceu ao longo dos anos e como o alcance da internet tomou proporções imensas, concomitantemente ao aumento da quantidade de usuários. Nesse diapasão, não somente ocasionou inúmeras vantagens para a sociedade, mas também proporcionou vulnerabilidades para a ocorrência de diversas condutas criminosas novas com potencial de ocasionar danos irreversíveis às vítimas.

Diante desse cenário, a legislação está em constante evolução para se adaptar aos novos crimes da internet, ou seja, a evolução da sociedade por meio da tecnologia tornou de extrema importância a análise e a tipificação dos atos cometidos pelo meio virtual, porém, é inegável a dificuldade dos legisladores em regulamentar tais atos, bem como, os direitos e os deveres dos usuários da rede.

Nos últimos tempos, o mundo tem assistido a uma ameaça crescente desses ataques, o que nos leva a um questionamento imediato. A legislação pátria e as ferramentas de informação são eficientes e suficientes na prevenção e combate aos crimes cibernéticos? Para além disso, os usuários das redes estão informados no tocante a prevenção na utilização da internet?

Apesar da iniciativa de punição contra os cibercrimes na legislação atual, tais regulamentações ainda não são suficientes para abranger todos as condutas cometidas na competência do ambiente virtual e garantir a segurança dos usuários.

Além do mais, a sociedade atual distribui riscos, ou seja, se autocolocam em posição de vulnerabilidade devido à diversos fatores e, ao mesmo tempo, essa mesma sociedade clama por segurança contra os riscos inerentes às situações da vida, como quando escolhem por aderir seguros de vida, planos de saúde, entre outros.

Nesse contexto, na medida que desenvolvem essas prevenções no ambiente físico, por consequência ocorre a diminuição dos riscos de insolvência. Dito isso, surge a necessidade de

implantar essa mesma prevenção do ambiente físico para os meios virtuais, ou seja, é necessário, como requisito essencial, uma conduta preventiva dos usuários aos riscos cibernéticos.

Em outras palavras, ao mesmo passo que na vida real as pessoas se previnem dos crimes cotidianos, no ambiente cibernético não deve ser diferente. Porém, com a falsa sensação de segurança que a internet proporciona, a maioria dos usuários ignoram ou desconhecem os riscos e, portanto, muitas vezes depreende-se condutas negligentes das vítimas cibernéticas.

Isto porque, nos dias atuais os usuários praticamente têm alegria em renunciar à sua privacidade, na medida em que distribuem seus dados em qualquer site de maneira deliberada e sem segurança, quando compartilham sua rotina nas redes sociais, quando clicam em qualquer link oferecido, entre outros exemplos que demonstram o descuido e despreparo dos usuários.

Por conseguinte, os cibercriminosos se beneficiam da inevitabilidade do uso da internet no cotidiano dos brasileiros, bem como, da falta de expertise que muitos usuários possuem em relação aos perigos do espaço cibernético. Assim, evidente afirmar que os usuários brasileiros não estão nem perto de estarem devidamente protegidos.

Vale ressaltar a impossibilidade da onipresença do Estado quanto a todas as atitudes da sociedade no ciberespaço ou em atuar frente a ausência do dever de cuidado das vítimas, uma vez que, se autocolocam em risco diariamente.

Logo, observa-se as consequências na medida em que os ataques cibernéticos têm se intensificado cada vez mais, em especial, diante dos usuários particulares por meio de diversas táticas que, inclusive, se renovam rapidamente e atingem grande percentual de sucesso.

Dessa forma, é imprescindível ter consciência de que hoje todos podem ser alvos, além do mais, a vítima cibernética tem condição especial, já que submete seus bens jurídicos, definindo seu grau de interação e exposição no ambiente cibernético, ou seja, é a única que pode incorporar instrumentos de autoproteção aos seus bens jurídicos na rede.

Indubitável a necessidade de uma análise criteriosa sobre o tema, uma vez que as informações nas redes são perigosas por si só e, somado a isso, os instrumentos formais e a conduta dos usuários de proteção e prevenção praticamente não existem.

A presente pesquisa possui como escopo contextualizar a ocorrência dos crimes cibernéticos e a compreensão do tema enquanto do aspecto jurídico, teórico e principalmente prático, de modo a ressaltar os perigos causados por um regramento insuficiente, bem como, pela insipidez dos usuários nas redes. Logo, pretende-se enfatizar a necessidade de uma postura preventiva.

Nessa esteira, busca-se, com o presente trabalho, dissecar o tema, analisando a prevenção individual de casa usuário, discorrendo sobre os limites jurídicos e observando os mecanismos disponíveis para a sociedade da informação.

A problemática primordial do estudo se insurge diante das condutas preventivas eficientes no combate a essa natureza de infração e que são ignoradas pela grande maioria dos usuários da rede, notoriamente ainda não tutelada suficientemente pelo ordenamento jurídico, bem como, pela impossibilidade de onipresença dos órgãos coercitivos para com a defesa dos crimes cibernéticos.

A realização da presente pesquisa foi baseada em pesquisa de cunho bibliográfico, por meio de doutrinas, documentos, artigos, a fim de tomar nota das opiniões sobre o assunto. Restou evidenciado o crescimento recorrente dos índices dessa modalidade criminosa, bem como, a desinformação e despreparo dos usuários da rede.

2. LEGISLAÇÃO BRASILEIRA ACERCA DOS CRIMES CIBERNÉTICOS

Uma análise da sociedade atual, mesmo que superficial, demonstra a grande mudança tecnológica e conduz para a conclusão da necessidade de aprimoramento da legislação penal informática, com o propósito de evitar à impunidade dos crimes praticados no ambiente virtual.

Em outras palavras, depreende-se a necessidade de o ordenamento jurídico pátrio estar em conformidade com os avanços da era digital. Porém, é notória a dificuldade de adaptação do Governo dentro deste contexto, na medida em que não consegue acompanhar o frenético avanço proporcionado pela internet.

Não se pode olvidar que, nos últimos anos, encontra-se alguns avanços no âmbito legislativo, em que foi produzido importantes ferramentas de proteção e combate aos crimes cibernéticos, conforme será desenvolvido a seguir.

Portanto, o objeto desse capítulo é elucidar a legislação atual relacionada aos crimes cibernéticos, demonstrando sua evolução para com os avanços da tecnologia, sua importância e o seu impacto na sociedade cibernética.

2.1. Lei Carolina Dieckmann – Lei n° 12.737/2012

Há dez anos entrava em vigor a Lei n° 12.737/2012, conhecida como Lei Carolina Dieckmann, a primeira legislação criada para punir os crimes informáticos e proteger as

informações e os dados individuais no ambiente digital, a qual promoveu algumas alterações no Código Penal formalizando e tipificando os chamados “crimes ou delitos cibernéticos”. Sua redação prevê os crimes oriundos do uso indevido de informações e materiais pessoais no tocante à privacidade de uma pessoa na internet.

Isto porque, a referida lei ganhou notoriedade e ficou conhecida pelo nome da atriz em razão da repercussão do crime contra honra cometido por meio da internet oriundo da invasão ao seu dispositivo e suas informações pessoais e íntimas subtraídas, inclusive com a divulgação na internet que rapidamente se espalharam pelas redes sociais.

Assim, um importante marco na legislação brasileira representando significativa mudança no ordenamento jurídico, haja vista tratar-se de crimes cada vez mais constantes na sociedade moderna, bem como, pela tipificação de condutas que não eram previstas como infração penal. Ou seja, antes de 2012 o acesso a dispositivos privados não era configurado crime, logo, a invasão da privacidade no ambiente cibernético era uma prática impunível. Com a Lei, a referida prática passa a ser tratada como crime.

Torna-se, portanto, uma valiosa ferramenta para zelar pela segurança e privacidade online. Inaugurando, assim, a evolução da legislação nesse sentido, na medida em que induz a reflexão da necessidade de um aprimoramento da legislação penal informática.

2.2. Marco Civil da Internet – Lei n° 12.765/2014

No Brasil, diante dos impactos causados nos interesses de diversos temas que ainda estavam em aberto com relação ao ambiente virtual, surge a Lei n° 12.965/2014, conhecida como o Marco Civil da Internet (“MCI”) que, até sua criação nenhum outro dispositivo legal estabelecia, com rigor, garantais, direitos e deveres para os usuários da rede.

Em resumo, possui três principais elementos estruturais: a neutralidade da rede, a liberdade de expressão e a privacidade. Introduziu conceitos a fim de garantir a proteção dos direitos dos usuários da rede relativos à privacidade e à proteção de dados, bem como, estabeleceu regras de armazenamento de dados por parte dos provedores de conexão de Internet.

O respeito à liberdade de expressão trazida pelo legislador retrata sua preocupação em criar um diploma legal em consonância com a Constituição Federal de 1988, que possui como fundamento o tema em questão em seu artigo 5°, inciso IX, bem como, enfatiza que o uso da internet pode e deve ser utilizado como forma de promoção à cidadania.

Outrossim, a discussão em torno do Marco Civil da Internet está constantemente presente no Supremo Tribunal Federal e com projeto em tramitação na Câmara dos Deputados

referente ao Projeto de Lei da Fake News, em especial, tratando sobre a tipificação do crime de divulgação em massa de mensagens com conteúdos inverídicos nas redes.

A necessidade de proteger a segurança e a privacidade de comunicação é um dos pontos mais importantes que a Lei apresenta, ou seja, visa principalmente à garantia da qualidade do acesso e privacidade dos usuários.

Logo, existe o entusiasmo para uma espécie de melhorias das regulações dos critérios para o controle de conteúdo que é feito pelas plataformas e meios de comunicações digitais. Há um caminho lento para o fortalecimento legislativo da proteção dos usuários nas redes? Sem dúvidas, mas existe.

2.3. Lei Geral de Proteção de Dados Pessoais – Lei n° 13.709/2018

Em 18 de setembro de 2020 entrou em vigor a Lei Geral de Proteção de Dados Pessoais, impactando as mais diversas áreas da sociedade brasileira. Isto porque, os usuários estavam constantemente e excessivamente expostos a danos decorrentes do conhecimento em massa sobre seus hábitos, preferências, informações pessoais sensíveis, entre outras. Logo, notória a necessidade de regulação dessa atividade, ou seja, necessidade de novas normas de proteção da privacidade para evitar que haja abusos no tratamento dos dados dos usuários.

Conforme se extrai do texto legislativo, tem como escopo versar sobre o tratamento dos dados pessoais a fim de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. O verbo “proteger” se faz presente com o intuito de destacar a vulnerabilidade dos titulares dos dados na relação com os agentes responsáveis pelo tratamento e armazenamento destas.

São diversos casos de tratamento ilegal ou inadequado dos dados pessoais, causando danos consideráveis e irreparáveis aos usuários, como nos casos de vazamento e venda de dados pessoais ou o compartilhamento com terceiros não autorizados. Clara violação aos direitos fundamentais assegurados pela Constituição Federal, uma vez que trata-se de invasões de privacidade oriundos de acessos privilegiados não autorizados dos dados obtidos.

Além disso, com o vazamento, comércio e compartilhamento não autorizado dos dados pessoais, os cibercriminosos também podem utilizar para aplicação de golpes dos mais variados tipos. Ilustra-se o importante caso do vazamento de dados com informações pessoais de 223 milhões de brasileiros, com isso, dezenas de arquivos foram disponibilizados publicamente e colocados à venda nas redes. Por óbvio, causando diversos impactos negativos para a segurança dos usuários da internet.

O respeito à privacidade evidenciado pelo legislador invoca outro fundamento constitucional, tão importante quanto, pautado no direito à liberdade, no qual mantém o usuário no controle dos limites ao tratamento de suas informações pessoais. Em outras palavras, o tratamento dos dados não pode ser contrário aos princípios fundamentais da privacidade e da liberdade, bem como, a segurança da informação disponibilizada nas redes deve ser assegurada desde a coleta.

2.4. Convenção de Budapeste – Decreto n° 11.491/2023

A Convenção sobre Crime Cibernético foi aberta para assinatura no ano de 2001, em Budapeste, tendo sido ratificada por 68 Estados, membros e não membros do Conselho da Europa, bem como, outros 158 países utilizam como orientação para suas legislações nacionais de combate aos crimes cibernéticos. Vale ressaltar que, trata-se da primeira Convenção Internacional de Cooperação Mundial de combate aos crimes cometidos no ambiente virtual com uma política criminal comum entre os países.

A República Federativa do Brasil ratificou e aderiu em 2021 por meio do Decreto Legislativo n° 37/21 e a promulgou internamente recentemente com o Decreto n° 11.491/2023, se tornando oficialmente signatário da Convenção. Sua adesão ao ordenamento jurídico brasileiro era necessária, tendo em vista, principalmente, a dispersão de informações e a dificuldade de geolocalização dos cibercriminosos.

A referida promulgação no território brasileiro assegura a ampliação de ferramentas legais de combate aos crimes informáticos, tendo em vista que esse tipo de criminalidade no ambiente virtual, não respeitam fronteiras. Ou seja, o Brasil entra na luta internacional contra os crimes cibernéticos, comprometido em garantir a segurança cibernética global.

Entretanto, a aceitação das obrigações internacionais para o combate dos cibercrimes não basta, sendo essencial medidas internas legislativas para tornar efetiva a segurança jurídica e, ao mesmo tempo, se adaptar à constante evolução tecnológica. Isto porque, passados mais de 20 anos desde a sua criação na ordem internacional, a Convenção ainda se mantém relevante e atual, uma vez que diversos temas no tocante a criminalidade cibernética está em evidência, como os golpes virtuais, os vazamentos de dados, a disseminação das *fake news*, entre outros.

Nota-se a criação e adoção de uma legislação apropriada para promoção da cooperação internacional, com o intuito prioritário de uma política criminal destinada à proteção da sociedade mundial contra os riscos associados ao uso da internet, a fim de facilitar a

investigação, a descoberta da autoria e julgamento desses delitos virtuais, estipulando conceitos de mútua compreensão e mecanismos internacionais para uma cooperação célere e confiável.

Diversas condutas são trazidas pela Convenção de Budapeste a serem criminalizadas pelos países signatários, definindo infrações criminais, cooperação internacional em investigações e a criação de leis para coibir atividades criminosas. Isso inclui a criação de unidades especializadas de investigação para troca de informações entre as autoridades internacionais competentes e a cooperação para extradição de suspeitos de crimes cibernéticos.

Para Carolina Yumi, diretora do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI) do Ministério da Justiça e Segurança Pública (MJSP):

> A integral implementação da Convenção de Budapeste no Brasil trará resultados positivos ao país, uma vez que ensejará a modernização de normativos e políticas adotadas na temática de enfrentamento aos crimes cibernéticos, assim como na coleta e preservação das provas digitais. [1]

Partindo de uma expectativa baseada na Convenção, há um entusiasmo de que a Convenção de Budapeste irá, progressivamente, encorajar as investigações diante da modernização do combate aos crimes cibernéticos, bem como, impulsionar o Brasil a dar continuidade ao seu desenvolvimento legislativo diante do contínuo avanço da cibercriminalidade.

3. CARACTERÍSTICAS E EVOLUÇÃO DOS CRIMES CIBERNÉTICOS

A evolução da tecnologia é cada vez mais presente na sociedade e o uso da internet se tornou indispensável no cotidiano das pessoas, bem como, uma ferramenta incrível de substituição dos atos físicos pelos atos virtuais. Com toda essa inovação e acessibilidade, simultaneamente houve diversas benesses, assim como problemáticas, como a criminalidade virtual, caracterizando um grande desafio para a ciência jurídica.

Por óbvio, antigamente a internet era bem diferente do que estamos usualmente acostumados nos dias de hoje. A ideia inicial para sua criação era o armazenamento de informações, bem como, para possibilitar que pessoas em diferentes espaços físicos pudessem

[1] YUMI, Carolina. **Convenção de Budapeste é promulgada no Brasil.** Ministério da Justiça e Segurança Pública. Publicado em 17 de abril de 2023. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil. Acesso em: 22 set. 2023.

se interligar. As últimas décadas foram fundamentais para que a internet ganhasse a forma que possui nos dias atuais.

A internet permaneceu por aproximadamente 20 anos sendo restrita ao âmbito acadêmico e científico, mas logo buscou-se maneiras para expandir esse uso para as demais atividades. Foi na década de 1990 que começava um esboço da internet para uso comercial, uma potente ferramenta com navegadores, possibilitando a realização de pesquisas em modo geral, encontrar livros, realizar compras e vendas sem sair de casa e a criação das famosas redes sociais, consequentemente acarretou o crescente número de usuários.

Com a criação das redes sociais, a internet alcançou um novo patamar de usabilidade e interação entre as pessoas do mundo todo. Atualmente, é quase impossível imaginar um mundo sem *instagram*, *facebook*, *whatsapp*, entre outros. Aplicativos esses que revolucionaram a sociedade digital mundial, em que as informações, notícias, acontecimentos, interações e a comunicação são simultâneas e descartáveis, tornando um vício para a maioria da população mundial, logo, é cada vez mais difícil ter controle sobre o mundo virtual.

Segundo a pesquisa TIC Domicílios realizada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br) em 2021, constatou que 81% da população tem acesso à internet, portanto, representa aproximadamente 152 milhões de pessoas. Assim, comparando com a pesquisa de 2019, o grupo de usuários de internet no país cresceu 7% em dois anos.[2]

Dito isso, o Brasil passou a ser um dos países que mais utiliza a internet, sendo o quarto país com mais usuários conectados do mundo. Por óbvio, é uma ferramenta que ajuda, auxilia e facilita a vida das pessoas, porém, o seu uso descontrolado, desenfreado e a maneira como se utilizam, dificultam o controle e a segurança nas redes. Assim como existem aqueles que utilizam o conhecimento para o bem, há também aqueles que utilizam para tirar proveito das novas situações e oportunidades que a internet proporciona, ensejando os crimes cibernéticos.

Atualmente é muito comum se deparar com a criminalidade cibernética, uma vez que esses criminosos acreditam que estão escondidos atrás de um computador ou, ainda, que a punição é praticamente inexiste. Ou seja, anos atrás ninguém poderia prever que a Internet poderia se tornar também uma “arma” poderosa para a prática criminal.

---

[2] SILVA, Victor Hugo**. 81% da população brasileira acessou a internet em 2021, diz pesquisa.** G1. Disponível em: https://g1.globo.com/tecnologia/noticia/2022/06/21/81percent-da-populacao-brasileira-acessou-a-internet-em-2021-diz-pesquisa.ghtml. Acesso em: 22 ago. 2023.

Assim posto, a relação dos ataques cibernéticos é extensa e podem ser dos mais variados tipos, desde crimes comuns contra particulares que acontecem com mais frequência até crimes contra Estados e grandes Corporações. Ilustra-se o ataque de invasão aos dados da empresa americana Sony Pictures, em um comunicado emitido em 2014, em que o especialista em segurança cibernética, Kevin Mandia, informou: "O malware era indetectável por programas antivírus comuns na indústria, e destruidor o suficiente para fazer com que o FBI emitisse um alerta para outras organizações sobre a ameaça."[3].

Além dos crimes já preconizados no ordenamento jurídico brasileiro, outras minudências vão surgindo atingindo aos mais diversos bens e interesses da sociedade. Conforme restou evidenciado anteriormente, a violação de bens jurídicos pode atingir desde o mais simples até o de mais alto escalão. Com isso, depreende-se a evolução alarmante desse tipo de criminalidade, com uma prioritária necessidade de combate, uma vez que os danos podem ser graves e irreversíveis.

4. VITIMOLOGIA E VITIMODOGMÁTICA

Antes do mais, a expressão "vitimologia" alcançou relevância com o trabalho "The Criminal an his Victim" de 1948 de Hans von Hentig. É o que nos ensina:

> Hentig propôs uma abordagem dinâmica, interacionista, desafiando a concepção de vítima como ator passivo. Salientou que poderia haver algumas características das vítimas que poderiam precipitar os fatos ou condutas delituosas. Sobretudo, realçou a necessidade de analisar as relações existentes entre vítima e agressor. [4]

Atualmente, a vitimologia tornou-se um campo de estudo orientado para formulação de políticas públicas, bem como, não deve mais ser entendida somente em termos de direito penal, mas também de direitos humanos, tendo em vista que a questão central da vitimologia trata-se do estudo das consequências das violações contra os direitos humanos.

Nesse sentido, a vitimologia vem, efetivamente, conferir uma nova concepção ao conceito de vítima, contribuindo para redefinir suas relações, posto que a vítima já não

---

[3] FOLHA DE SÃO PAULO. ROMANI, Bruno. **Entenda o caso da invasão hacker à Sony Pictures.** Disponível em: http://www1.folha.uol.com.br/tec/2014/12/1562817-entenda-o-caso-da-invasao-hacker-a-sony-pictures.shtml. Acesso em: 19 ago. 2023.

[4] MENEZES, CRISTIANO. Instituto Marconi. **Noções de Criminologia.** Docero Brasil. 13 de março de 2020, p. 27. Disponível em: https://doceru.com/doc/ne1n858. Acesso em: 17 de ago. de 2023.

corresponde apenas ao sujeito passivo. Com isso, identifica-se no crime uma espécie de transação, em que o infrator e a vítima desempenham papéis.

Sendo assim, os estudos da vitimologia proporcionam extensa contribuição para melhor enfrentamento do fenômeno da criminalidade, em especial, a partir do enfoque da interação infrator-vítima, ou seja, em qual proporção a vítima interfere para o surgimento da ação ou em que medida suas ações condicionam ou direcionam as ações do infrator cibernético.

O desempenho da cibercriminalidade, a legislação vigente e a constante atualização das ferramentas técnicas de segurança digital tornam forçoso a análise do papel social da vítima, bem como, da sua autocolocação em risco, surgindo a ideia de autoproteção.

Portanto, a análise sobre a vítima também se faz pertinente para a prevenção do delito, uma vez que a vítima é fonte de informações, logo, é certo que a vítima, suas características e condutas são elementos e fatores relevantes para o adequado funcionamento do combate aos crimes cibernéticos.

O conceito introdutório da chamada "prevenção vitimaria", enfatiza a importância de se evitar que os delitos aconteçam a partir da reorientação às vítimas, para que adotem condutas e perspectivas adequadas e, consequentemente, reduzam ou eliminem as situações de risco. Tal reflexão do referido conceito parte da ideia de que o crime cibernético é um fenômeno seletivo, ou seja, atinge os mais vulneráveis, as vítimas mais propensas.

Assim, essa prevenção vitimaria exige adoção de políticas públicas sociais, ensejando intervenção e participação social. Finalmente, co-responsabiliza todos. O que é muito correto, já que todos deveriam ter a consciência de que hoje vivemos em uma sociedade de risco.

Nesse contexto, é necessário direcionar as reflexões sobre a vítima cibernética de acordo com os pensamentos vitimodogmáticos com o objetivo de observação e correção na concepção de vigência da norma. Destaca HASSEMER (1990), "a norma jurídico-penal só tem oportunidade de ter vigência prática se encontra uma vítima atenta e disposta à proteção" [5]

Por conseguinte, a violência cibernética não é somente um problema do Estado e os esforços no seu combate não devem ser direcionados apenas ao infrator. Falar sobre o combate a tal criminalidade é falar, principalmente, em prevenção. E a melhor forma de combater e diminuir a criminalidade é alcançando o crime em suas causas, suas raízes e não nas suas consequências.

---

[5] HASSEMER, Winfried. **Consideraciones sobre la víctima del delito.** Anuario de Derecho Penal y Ciencias Penales. Madrid, v. 43, n. 1, p. 241-259, 1990.

Por fim, diante do exposto, a população deveria ser reeducada para o exercício da cidadania em dois sentidos: direitos e deveres. Trata-se da prevenção a partir da vítima, a partir da consciência do papel ativo da vítima na dinâmica dos delitos informáticos.

5. AUTOCOLOCAÇÃO EM RISCO DA VÍTIMA NAS REDES

Inicialmente, vale elucidar que, a vítima tem um papel diferenciado no ambiente cibernético, eis que a sua conduta possui especial relevância não só para as consequências dos crimes como para sua prevenção. Assim, a ideia de passividade da vítima é substituída no ciberespaço, por um comportamento dinâmico, complexo e ativo, caracterizador de uma posição que influencia no aumento ou implemento, por si só, do risco ao bem jurídico submetido nas redes.

Ao contrário do que ocorre no ambiente físico, no ambiente virtual o cibercriminoso não escolhe a vítima ao mero acaso, alguns fatores interferem no momento da escolha de quem será a vítima. Spencer Toth SYDOW (2013) disciplina que "a vítima é um sujeito de foco adequado, um alvo que se mostra preferencial seja por quem é, por como se porta, por o que possui ou por onde está" [6].

Plausível ilustrar descrevendo um exemplo simples, mas didático, da seguinte situação hipotética: Uma garota realiza uma publicação nas suas redes sociais de uma foto sua no parque perto da sua casa com o seu colar de ouro no pescoço. Quais as consequências possíveis? De acordo com o mundo cibernético, aquela garota com apenas um clique, possibilitou que milhares de pessoas tenham acesso a tal informação simultaneamente, em que qualquer infrator consegue saber exatamente sua localização, horário, vestimenta e acessórios para efetuar o fato delitivo, seja ele qual for.

Ou seja, a princípio, não há problema em apenas compartilhar momentos nas redes. Porém, não é tão simples. O momento da postagem dos "stories" ou "posts" nas redes sociais, propiciou ao infrator a oportunidade esperada. Supondo que ocorra o delito, ele poderia ter sido evitado com uma conduta preventiva? Certamente. Nesse caso, bastaria a consciência de que todas as informações são perigosas por si só, logo, esperar para compartilhar a informação de um outro lugar seguro, seria simples e eficaz.

---

[6] SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas.** São Paulo: Saraiva, 2013.

Mostra-se necessário a consciência e preocupação com as informações compartilhadas em tempo real nas redes. Parece simples e, para alguns até óbvio, mas isso não ocorre na prática, eis que nos deparamos com usuários desinformados e despreocupados regularmente.

Vale ressaltar neste exemplo hipotético que, a informação disponibilizada pela vítima nas redes contribuiu para que ocorresse o fato delitivo no mundo real, físico. Logo, percebe-se a imensurável quantidade de delitos que podem surgir com a vítima desatenta, seja no ambiente virtual, seja no ambiente físico.

Atualmente, em especial os jovens, quantos se preocupam com as informações compartilhadas nas redes sociais? A minoria. Logo, não podemos deixar de considerar que trata-se de algo que controlamos, ou melhor, que somos capazes de evitar, de prevenir. Porém, são inúmeros exemplos reais de casos análogos que demonstram com exatidão a falta de conscientização da vítima nas suas condutas e comportamentos nas redes que, muitas vezes, facilita o ato ilícito.

Compreende-se que o espaço cibernético é um ambiente de criminalidade novo e distinto do físico que, não é a vontade do criminoso que irá determinar a atividade criminosa, mas sim a interação concreta com a vítima que acaba por proporcionar a lesão ao seu bem jurídico de maneira indireta.

Comparando com o ambiente físico, as pessoas não saem de suas casas, em uma localidade “perigosa”, deixam a porta aberta com um bilhete: volto daqui 2 horas. Muito pelo contrário, a maioria possui diversas fechaduras, alarmes e até seguros. É dessa conduta preventiva que tratamos, que é necessária existir no ambiente cibernético, bem como, é extremamente necessário a participação, disposição e preparo da sociedade. Ou seja, somente a legislação jamais será suficiente para garantir a segurança dos usuários no ciberespaço.

6. RISCOS NO CIBERESPAÇO À LUZ DA NEGLIGÊNCIA DA VÍTIMA DIGITAL

Conforme exposto, a internet segue impactando as relações sociais e criando novas maneiras de cometer crimes, sendo, em verdade, uma projeção do que se passa no mundo material. Logo, no ambiente físico possuímos o conhecimento das medidas preventivas para, muitas vezes, prevenir alguns delitos.

No ambiente cibernético, é notório o número crescente de usuários e, especialmente, a população de analfabetos virtuais, em que se faz necessário também essa projeção de condutas preventivas do meio físico para o meio virtual.

O Bittencourt defende que:

> Se por um lado a tecnologia dá aos usuários ampla liberdade e máxima igualdade individual, por outro lado ela lhes retira a habilidade de distinguir as pessoas com as quais se relacionavam virtualmente, além de lhes restringir a capacidade de diferenciar a sensação de segurança da ideia de segurança como realidade. [7]

As principais razões que deram ênfase a necessidade de uma nova ótica em relação à prevenção são (i) o aumento dos cibercrimes e o surgimento constante de novas formas de cibercriminalidade; (ii) baixa porcentagem de solução do delito; (iii) insegurança cada vez maior dos usuários e (iv) as consequências e repercussões do delito na sociedade, entre outras.

Isto porque, há carência dos usuários conectados, como a falta de informação e conhecimento nesse setor e a relativa ausência de participação na prevenção do delito, em que os criminosos cibernéticos procuram oportunidades regularmente para se beneficiar da falta de conhecimento dos usuários do que é novo, já que têm a errada impressão que o anonimato é possível nas redes e que a internet é uma "terra sem lei".

Os usuários estão sendo projetados socialmente para "clicar aqui", ou seja, cada vez mais ludibriados pelo crime cibernético, ensejando cada vez mais conscientização, porém, ainda, os usuários continuam sendo negligentes.

Por que somos negligentes nas redes? De acordo com Joseph Labrie, professor adjunto de Psicologia da Loyola Marymount University e PhD, trata-se da "impotência aprendida", conforme disciplina:

> A impotência aprendida ocorre quando as pessoas não sabem o suficiente sobre um problema ou não sabem como solucioná-lo. É como ser extorquido em uma oficina mecânica – se você não sabe o suficiente sobre carros, não discuta com o mecânico. As pessoas simplesmente aceitam as situações, mesmo que se sintam mal. [8]

De acordo com o Relatório de Crimes Cibernéticos da empresa norte americana Norton baseado na pesquisa com 7.066 adultos entrevistados de 14 países diferentes realizada pela empresa Symantec Corporation, demonstra que 76% dos adultos já foram vítimas de algum tipo de crime cibernético, quase um terço das vítimas (31%) nunca solucionaram um crime cibernético e, ainda, para quase três em dez vítimas (28%) afirmam que o maior incômodo é o

---

[7] BITTENCOURT, Rodolfo Pacheco Paula. **O anonimato, a liberdade, a publicidade e o direito eletrônico**. 2016, Disponível em: https://rodolfoppb.jusbrasil.com.br/artigos/371604693/o-anonimato-a-liberdade-a-publicidade-e-o-direito-eletronico. Acesso em: 03 out. 2023

[8] LABRIE, Joseph. **Relatório de Crimes Cibernéticos NORTON: O Impacto Humano**. SYMANTEC, Norton. p. 7. Disponível em: https://docplayer.com.br/1488607-Relatorio-de-crimes-ciberneticos-norton-o-impacto-humano.html. Acesso em 10 set. 2023.

tempo que leva para resolver. Resta evidenciado que as pessoas normalmente preferem não resolver, preferem evitar o stress, a raiva e o constrangimento. Dito isso, notória a existência de um dilema em relação ao comportamento online dos usuários.

Os usuários resistem estranhamente protegerem a si mesmas e seus computadores dos riscos cibernéticos porque acham muito difícil e complexo.

6.1. Consequências

O caráter global da internet e a ausência de um domínio único sobre suas dimensões impõem a reflexão acerca dos efeitos e consequências do mundo virtual para o mundo real, físico. Dito isso, à pouca informação e instrução da população no que toca à utilização e navegação na internet, ensejam para um forte crescimento de sujeitos passivos nos crimes virtuais.

Logo, as vítimas cibernéticas são ainda mais vulneráveis, notadamente porque, além da relativa ausência de tutela e atraso legislativo para com o avanço tecnológico, desfrutamos de um ambiente extremamente perigoso, onde o cibercriminoso no cometimento do delito, vale-se do anonimato e da sensação de segurança e impunidade.

Além do mais, a facilidade com que as pessoas têm acesso aos conteúdos íntimos e dados de terceiros vem provocando frequentes violações aos direitos da personalidade. Nos últimos anos, lesões à privacidade, à honra, ao nome e à imagem do indivíduo vêm ocorrendo de forma exponencial.

A internet é considerada atualmente o mais benéfico instrumento já desenvolvido, proporcionando facilidades e recursos inimagináveis, porém, não são só vantagens, a liberdade nas redes tem um custo o qual não é muito agradável, a perda da privacidade oriunda da falta de segurança nas redes. Vale ressaltar que trata-se de uma problemática mundial, em que todas as informações submetidas no espaço cibernético podem estar comprometidas, de modo que nenhum pais até hoje encontrou alguma solução.

6.2. Educação Digital

A prevenção do delito é uma tendência atual, isto é, existe um consenso generalizado em considerar que a prevenção do delito constitui um objetivo importante, eis que, é melhor prevenir o crime do que reprimi-lo.

Na atualidade e na presente temática, compreender a dinâmica criminal não significa apenas identificar os espaços dos crimes, dos criminosos e suas características para ações repressivas, bem como, é nítido a imprecisão e a ineficiência dos órgãos estatais de repressão. Significa, antes de tudo, entender os processos e condutas próprias para antecipar-se à sua ocorrência, prevenindo-o.

A Moderna Criminologia está se consolidando como um empreendimento interdisciplinar, sugerindo estratégias de prevenção inovadoras e ousadas que vão além do cibercriminoso, que atinjam as vítimas e o espaço cibernético. Portanto, sua prevenção deve se pautar em políticas que intervenham positivamente na relação do usuário com a rede que são, principalmente, conscientizar os usuários sobre segurança cibernética e outros serviços que valorizem a cidadania.

Sob essa ótica, políticas públicas só poderão ser formuladas com o apoio de movimentos sociais, instituições, universidades, comunidade em geral. Logo, a prevenção deve ser comunitária, ou seja, a comunidade será reeducada para o exercício da cidadania cibernética.

Isto porque, em regra, a conexão com a internet influi psicologicamente na vítima, pois ocorre de um ambiente em que o usuário sente-se fisicamente seguro, como de sua casa ou de seu trabalho, ensejando a falsa sensação de segurança no meio virtual, influenciando para que naveguem com menor cautela e responsabilidade, como abrindo e-mails e páginas desconhecidas, entrando pelos sites de forma despreocupada e até fazendo compras, disponibilizando seus dados pessoais, bancários, entre outras.

Outrossim, com tantos dados disponíveis para os cibercriminosos diante da grande quantidade de dados pessoais vazados no ambiente cibernético, é necessário estar constantemente vigilante, pois as tentativas de fraudes com os dados obtidos são recorrentes.

Embora haja entusiasmo por parte de legislação, na prática, esses direitos positivados nem sempre são garantidos, por isso, a melhor maneira de combate para esse tipo de crime ainda é a prevenção. Salienta CRESPO (2013, p.107) “a sociedade de risco exige maior conscientização por parte de seus integrantes, sendo este o preço da modernidade e dos avanços tecnológicos”[9].

Para corroborar, o consultor líder de segurança cibernética da empresa norte americana Norton, Adam Palmer, pronunciou:

> Todos nós deveríamos poder desfrutar da Internet sem medo de nos tornarmos vítimas. O apoderamento ocorrerá aumentando-se a conscientização dos assuntos

[9] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais.** São Paulo, Saraiva, 2011.

> relacionados ao crime cibernético e educando as pessoas sobre as melhores práticas, produtos e tecnologias corretos para prevenir que nos tornemos vítimas."[10]

Nem todos os usuários conhecem os deveres para garantir a segurança cibernética, sendo necessário uma conscientização da conduta preventiva, uma expectativa social para que todas as pessoas dotadas de meios para proteger seus bens jurídicos informáticos, o façam. Ou melhor, que as pretensas vítimas mantenham-se em estágios ótimos de autopreservação.

7. CONSIDERAÇÕES FINAIS

No presente estudo, foi possível discorrer sobre a complexidade dos avanços tecnológicos, seus reflexos na vida social atual e como isso propiciou para o aparecimento de novas condutas criminosas, bem como, de velhos tipos penais que ganharam novos formatos, desencadeando um novo olhar e conduta para com o espaço cibernético, demonstrando o perigo que é a associação da tecnologia com a delinquência.

Ou seja, aproveitando-se da rapidez tecnológica e da lentidão burocrática das entidades coercitivas estatais, os cibercriminosos se estruturaram e aumentaram cada vez mais o volume de delitos informáticos, ensejando a conduta preventiva perpetrada no presente estudo.

Compreende-se que o tema abordado é de imensa relevância para o Direito, eis que os crimes cibernéticos se tornaram um surto digital global silencioso, sua extensão é alarmante e as ações falhas são frequentes. Logo, de suma importância estudar os aspectos vitimológicos que existem por trás desses delitos, delinear as características das vítimas, sua nova concepção e como influência para os riscos inerentes ao espaço cibernético.

Além disso, crucial a constante atualização legislativa do Direito Penal com a nova realidade que vive a população, a famosa era digital. Ou seja, embora notório o avanço do ordenamento jurídico brasileiro nessa temática, ainda há muito que se fazer, tendo em vista que os cibercrimes evoluem simultaneamente com a própria tecnologia. Logo, se faz necessário uma perfeita harmonia do poder legislativo, judicial e da sociedade para combate desses delitos informáticos.

---

[10] PALMER, Adam. **Relatório de Crimes Cibernéticos NORTON: O Impacto Humano**. SYMANTEC, Norton. p. 7. Disponível em: https://docplayer.com.br/1488607-Relatorio-de-crimes-ciberneticos-norton-o-impacto-humano.html. Acesso em 10 set. 2023.

Noutro ponto, com a evolução constante do mundo informático, nos deparamos com uma sociedade desinformada, despreocupada, que clamam por segurança ao mesmo passo que, se autocolocam em risco. Por óbvio, não há proteção e vigilância absoluta, mas o conhecimento sobre as ameaças reduz o risco dos crimes se concretizarem, ou seja, a prevenção se apresenta como a melhor "arma" nesse combate, sendo o modo de reeducar os usuários para o uso racional nas redes, para se navegar de forma segura.

É certo que os crimes cibernéticos não irão desaparecer, mas podem ser combatidos e prevenidos se a sociedade for reeducada, ativa e consciente neste sentido. Sendo imprescindível diminuir os riscos, evitar o evitável, com a crescente preocupação e cuidado dos usuários em adquirir uma conduta preventiva no ciberespaço.

Portanto, evidencia-se no presente estudo que cada clique importa e que a necessidade de conscientização e educação por parte de todos os usuários conectados é inadiável, com o intuito de retomar a Internet dos criminosos cibernéticos.

8. REFERÊNCIAS BIBLIOGRÁFICAS

ALTIERES, Rohr. **Megavazamento de dados expõe informações de 223 milhões de números de CPF.** 2021. G1. Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/01/25/vazamentos-de-dados-expoem-informacoes-de-223-milhoes-de-numeros-de-cpf.ghtml. Acesso em: 11 ago. 2023.

BITTENCOURT, Rodolfo Pacheco Paula. **O anonimato, a liberdade, a publicidade e o direito eletrônico.** 2016, Disponível em: https://rodolfoppb.jusbrasil.com.br/artigos/371604693/o-anonimato-a-liberdade-a-publicidade-e-o-direito-eletronico. Acesso em: 03 out. 2023.

Caderno de Pós-Graduação em Direito: Crimes Digitais. Coordenadores, Lilian Rose Lemos Rocha et al. – Brasília: UniCEUB: ICPD, 2020. Disponível em: https://www.repositorio.uniceub.br. Acesso em: 11 set. 2023.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais.** São Paulo, Saraiva, 2011.

FOLHA DE SÃO PAULO. ROMANI, Bruno. **Entenda o caso da invasão hacker à Sony Pictures.** Disponível em: http://www1.folha.uol.com.br/tec/2014/12/1562817-entenda-o-caso-da-invasao-hacker-a-sony-pictures.shtml. Acesso em: 19 ago. 2023.

HASSEMER, Winfried. **Consideraciones sobre la víctima del delito.** Anuario de Derecho Penal y Ciencias Penales. Madrid, v. 43, n. 1, p. 241-259, 1990.

HERNANDEZ, Erika Fernanda Tangerino; TOLEDO, Nathália Karina Abucci de. **Crimes Cibernéticos: seus efeitos revolucionários diante de uma legislação em constante evolução.** Revista Jurídica da UniFil, [S.l.], v. 17, n. 17, p. 72-84, set. 2021. ISSN 2674-7251. Disponível em: http://periodicos.unifil.br/index.php/rev-juridica/article/view/2424. Acesso em: 01 set. 2023.

JACON AYRES PINTO, Danielle; CARLOS FRANCISCO DOS SANTOS, José. **Internet: Dinâmicas da Segurança Pública e Internacional.** VI Encontro Virtual do CONPEDI. Florianópolis; CONPEDI, 2023. Disponível em: http://site.conpedi.org.br/publicacoes/4k6wgq8v/pk4u6114/ArGY2mnoJl42woTK.pdf. Acesso em: 06 out. 2023.

LABRIE, Joseph. **Relatório de Crimes Cibernéticos NORTON: O Impacto Humano.** SYMANTEC, Norton. p. 7. Disponível em: https://docplayer.com.br/1488607-Relatorio-de-crimes-ciberneticos-norton-o-impacto-humano.html. Acesso em 10 set. 2023.

Lei Geral de Proteção de Dados Comentada: com enfoque as relações e trabalho. Coordenação Selma Carloto, Mariana Almirão. 1. Ed. São Paulo: Ltr, 2021. Vários autores. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=3CE_EAAAQBAJ&oi=fnd&pg=PA13&dq=lei+geral+de+prote%C3%A7%C3%A3o+de+dados+preven%C3%A7%C3%A3o&ots=uDKUkEEy2M&sig=0jnkYCbPAyrzKHWb4S82O1RV-8Y&redir_esc=y#v=onepage&q=lei%20geral%20de%20prote%C3%A7%C3%A3o%20de%20dados%20preven%C3%A7%C3%A3o&f=false. Acesso em: 27 set. 2023.

MAURÍCIO FREIRE SOARES, Ricardo; DE ARAÚJO SANTOS, George. **O Marco Civil da Internet e a Tutela Consumerista no Ambiente Virtual.** Revista Amagis Jurídica, [S.l.],

v. 13, n. 1, p. 323-356, out. 2023. ISSN 2674-8908. Disponível em: <https://revista.amagis.com.br/index.php/amagis-juridica/article/view/271>. Acesso em: 28 out. 2023.

MENEZES, CRISTIANO. Instituto Marconi. **Noções de Criminologia.** Docero Brasil. 13 de março de 2020, p. 27. Disponível em: https://doceru.com/doc/ne1n858. Acesso em: 17 de ago. de 2023.

MURATA, Lumi Kamimura; D. A. M.; TORRES, Ritzmann, M. P. (2023). **A convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora?.** Boletim IBCCRIM, 31(368). Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/575. Acesso em: 05 out. 2023.

PALMER, Adam. **Relatório de Crimes Cibernéticos NORTON: O Impacto Humano.** SYMANTEC, Norton. p. 7. Disponível em: https://docplayer.com.br/1488607-Relatorio-de-crimes-ciberneticos-norton-o-impacto-humano.html. Acesso em 10 set. 2023.

SILVA, Victor Hugo. **81% da população brasileira acessou a internet em 2021, diz pesquisa.** G1. Disponível em: https://g1.globo.com/tecnologia/noticia/2022/06/21/81percent-da-populacao-brasileira-acessou-a-internet-em-2021-diz-pesquisa.ghtml. Acesso em: 22 ago. 2023.

SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas.** São Paulo: Saraiva, 2013.

YUMI, Carolina. **Convenção de Budapeste é promulgada no Brasil.** Ministério da Justiça e Segurança Pública. Publicado em 17 de abril de 2023. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil. Acesso em: 22 set. 2023.

TERMO DE AUTENTICIDADE DO TRABALHO DE CONCLUSÃO DE CURSO

Eu, Giovanna Monteiro Mendes discente regularmente matriculada na disciplina TCC II, da 10ª etapa do curso de Direito, matrícula nº 42072344, período Noturno, turma 10S, tendo realizado o TCC com o título: CIBERCRIMINALIDADE E NEGLIGÊNCIA DIGITAL: Autocolocação em risco da vítima sob a orientação da Professora Thamara Duarte Cunha Medeiros declaro para os devidos fins que tenho pleno conhecimento das regras metodológicas para confecção do Trabalho de Conclusão de Curso (TCC), informando que o realizei sem plágio de obras literárias ou a utilização de qualquer meio irregular.

Declaro ainda que, estou ciente que caso sejam detectadas irregularidades referentes às citações das fontes e/ou desrespeito às normas técnicas próprias relativas aos direitos autorais de obras utilizadas na confecção do trabalho, serão aplicáveis as sanções legais de natureza civil, penal e administrativa, além da reprovação automática, impedindo a conclusão do curso.

São Paulo, 07 de novembro de 2023.

Giovanna Mendes

Giovanna Monteiro Mendes