

**CENTRO DE ENSINO SUPERIOR LTDA CESREI
FACULDADE CURSO DE BACHARELADO EM DIREITO**

JANICLÉIA GOMES FERREIRA

**CRIMES VIRTUAIS: UMA REALIDADE OBSTACULADA POR UMA LEGISLAÇÃO
INEFICAZ E INCOMPLETA**

CAMPINA GRANDE - PB

2022

JANICLÉIA GOMES FERREIRA

**CRIMES VIRTUAIS: UMA REALIDADE OBSTACULADA POR UMA LEGISLAÇÃO
INEFICAZ E INCOMPLETA**

Trabalho de Conclusão de Curso
apresentado à Coordenação do Curso de
Direito da Faculdade CESREI, como
requisito parcial para a obtenção do grau
de Bacharel em Direito pela referida
instituição.

Orientadora: Dra. Gleick Meira Oliveira
Dantas

CAMPINA GRANDE - PB

2022

F383c Ferreira, Janicléia Gomes.
Crimes virtuais: uma realidade obstaculada por uma legislação ineficaz e incompleta / Janicléia Gomes Ferreira. – Campina Grande, 2022.
73 f. : il. color.

Monografia (Bacharelado em Direito) – Faculdade Reinaldo Ramos-FAAR – Centro de Educação Superior Reinaldo Ramos-CESREI, 2022.
"Orientação: Profa. Dra. Gleick Meira Oliveira Dantas".
Referências.

1. Crimes Virtuais. 2. Crime Digital – Vítimas. 3. Leis. 4. Legislação Ineficaz. I. Dantas, Gleick Meira Oliveira. II. Título.

CDU 343.63:004.738.5(81)(043)

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA SEVERINA SUELI DA SILVA OLIVEIRA CRB-15/225

JANICLÉIA GOMES FERREIRA

**CRIMES VIRTUAIS: UMA REALIDADE OBSTACULADA POR UMA LEGISLAÇÃO
INEFICAZ E INCOMPLETA**

Aprovada em: ____ de _____ de ____

BANCA EXAMINADORA

Professora Dra. Gleick Meira Oliveira Dantas
CESREI- Faculdade
(Orientadora)

Professor Me. Rodrigo Araújo Reul
CESREI- Faculdade
(1º Examinador)

Professor Me. Diego Araújo Coutinho
CESREI- Faculdade
(2º Examinador)

A Deus, aos meus pais, a minha família
DEDICO

AGRADECIMENTOS

A Deus por nunca ter me abandonado com sua infinita misericórdia e proteção divina livrando –me de todo mau que quis me deter. Obrigado Senhor!

Gratidão a minha guerreira e melhor amiga, minha mãe incomparável, que nunca mediu esforços sempre ajudando e me apoiando em todas as fases de minha vida.

Gratidão ao meu pai que sempre me ensinou o caminho certo a seguir com seu zelo e afeto por mim.

Obrigado por toda compreensão de minha família comigo, marido e filhos pois nunca foram motivos de empecilhos e desmotivação e sim de inspiração para continuar firme e forte.

Grata por todo apoio de parentes que juntos sabem minha história e torcem para que meus objetivos sejam alcançados.

Agradeço a todos os professores que de forma direta e indireta colaboraram nos ensinamentos acadêmicos dessa jornada e à CESREI, pelo apoio institucional.

Gratidão em especial a minha orientadora Gleick, que desempenhou seu papel com bastante eficácia e com total apoio e encorajamento contínuos na pesquisa deixando mais leve essa tarefa desafiadora.

Obrigado a todos que acompanharam essa minha trajetória e repassaram boas energias que foram revertidas em coragem para que esse sonho tenha se realizado com sucesso.

Obrigado de coração a todos vocês.

“O sucesso nasce do querer, da determinação
e persistência em se chegar a um objetivo.
Mesmo não atingindo o alvo,
quem busca e vence obstáculos,
no mínimo fará coisas admiráveis.”

(José de Alencar)

RESUMO

O presente trabalho tem como tema a realidade da ineficácia da legislação brasileira diante dos crimes virtuais. Onde o objetivo é abordar as lacunas existentes nas leis vigentes no Código Penal brasileiro, que acaba acarretando impunidade aos infratores responsáveis pelas condutas delituosas no mundo virtual e subsequentemente afeta o mundo real das vítimas. Para seu desenvolvimento, o presente trabalho foi desenvolvido por pesquisa bibliográfica, sendo caracterizado como qualitativo e descritivo. A escolha desse tema surgiu em busca de uma resposta como meio de orientação para que as pessoas tomem ciência de como devem agir diante de crimes virtuais e possam se proteger de tais delitos no propósito de uma análise das falhas deixadas nas previsões legais na virtualidade. Para tanto foi apresentado aspectos históricos da origem da internet, sua importância na sociedade, as modificações causadas com a tecnologia, aspectos comportamentais dos usuários, a realidade das vítimas que por descrença em conseguir resultados punitivos aos criminosos acabam desistindo de levar a diante as denúncias ou até mesmo por vergonha da situação já que afeta diretamente sua honra denegando sua imagem. O andamento jurídico indolente também é um fator que colabora para o aumento dos casos. Aspectos de prevenção e combate aos crimes virtuais devem ser vistos com um olhar minucioso de um cuidado especial afim de evitar danos irreparáveis as vítimas. Concluindo-se que, embora tenha havido progresso nas leis de combate aos crimes virtuais, elas não são suficientes para inibir o avanço que os criminosos usam nas técnicas tecnológicas para se inovar conforme a sua necessidade, e acabam ficando um passo à frente do poder legislativo.

Palavras-Chave: Crime Digital, Leis, Vítimas, Ineficaz, Realidade.

ABSTRACT

The present work has as its theme the reality of the ineffectiveness of Brazilian legislation in the face of virtual crimes. Where the objective is to address the existing gaps in the laws in force in the Brazilian Penal Code, which ends up leading to impunity for offenders responsible for criminal conduct in the virtual world and subsequently affects the real world of victims. The choice of this theme arose in search of an answer as a means of guidance so that people become aware of how they should act in the face of virtual crimes and can protect themselves from such crimes in the purpose of an analysis of the flaws left in the legal provisions in virtuality. In order to do so, historical aspects of the origin of the internet, its importance in society, the changes caused by technology, behavioral aspects of users, the reality of victims who, out of disbelief in achieving punitive results for criminals, end up giving up on carrying out the complaints or even out of shame about the situation as it directly affects his honor by denigrating his image. The indolent legal course is also a factor that contributes to the increase in cases. Aspects of preventing and combating cybercrimes must be seen with a meticulous look and special care in order to avoid irreparable harm to victims. The conclusion is that although there has been progress in the laws to combat cybercrime, they are still not enough to inhibit the advance that criminals use in technological techniques to innovate as needed, and end up staying one step ahead of power. legislative.

Keywords: Digital Crime, Laws, Victims, Ineffective , Reality.

LISTA DE ABREVIATURAS E SIGLAS

ARPA- Advanced Research Projects Agency

ARPANET- Advanced Research Projects Agency Network

Art. - artigo

ANPD- Autoridade Nacional de Proteção de Dados

BR- Brasil

BBC- British Broadcasting Corporation

CFAA- Computer Fraud and Abuse Act

DNA- Ácido Desoxirribonucleico

ECA -Estatuto da Criança e Adolescente

EUA- Estados Unidos da América

ENIAC - Eletric Numeric Integrator and Calculator

FNC- Federal Networking Council

GDPR- General Data Protection Regulation

GPS- Global Positioning System

ID- identity (identidade)

IP- Internet Protocol

KYC- know your customer ou conheça seu consumidor

LGBTQIA+- Lésbicas, Gays, Bissexual, Transgênero, Queer, Intersexo, assexual, mais.

LGPD- Lei Geral de Proteção de Dados

LINDB- Lei de Introdução às Normas do Direito Brasileiro

LICC- Lei de Introdução ao Código Civil

MCI- Marco Civil da Internet

NR- Norma Regulamentadora

n. - números

ONG-Organização Não Governamental

PLC- Projeto de Lei da Câmara

Pg. - Página

PL- Projeto de Lei

p.- Página

PIN- Personal Identification Number

RNP- Rede Nacional de Pesquisa

RENPAc- Rede Nacional de Comunicação de Dados por Comutação de Pacotes

RGPD- Regulamento Geral de Proteção de Dados

SWGfL -South West Grid for Learning

SF-Senado Federal

TOR- The Onion Router

TCP/IP -Protocolo de Controle de Transmissão/protocolo da internet (Transmission Control Protocol/Internet Protocol)

UE- União Europeia

USP- Universidade de São Paulo

UNIVAC- Universal Automatic Computer - Computador Automático Universal

WWW- World Wide Web

SUMÁRIO

INTRODUÇÃO	12
1 CAPÍTULO I - SÍNTESE HISTÓRICA DA INTERNET	14
1.1 INTERNET: DA ORIGEM AOS DIAS ATUAIS	14
1.2 SOCIEDADE DIGITAL	17
1.3 INTERNET NO BRASIL	19
1.4 REDES SOCIAIS NA INTERNET.....	22
2 CAPÍTULO II - CRIME DIGITAL	27
2.1 COMPETENCIA PARA PROCESSAR E JULGAR OS CRIMES VIRTUAIS	33
2.2 PROVAS	37
2.3 PUNIBILIDADE	40
2.4 PRINCÍPIO DA RESPONSABILIDADE PENAL SUBJETIVA E RESPONSABILIDADE DA PESSOA JURÍDICA	42
2.5 PRINCÍPIO DO NE BIS IN EADEM.....	43
2.6 PENAS	43
3 CAPÍTULO III - ESTRUTURAS LEGAIS NO ÂMBITO DIGITAL	46
3.1 O DIREITO DO CONSUMIDOR NA ERA DIGITAL.....	49
3.2 LEI 12.737/12 (LEI CAROLINA DIECKMANN)	50
3.2.3 Invasão de dispositivo informático.....	50
3.2.4 Ação penal	50
3.2.5 Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública	50
3.2.6 Falsificação de documento particular	51
3.3 LEI N. 12.965/2014 (MARCO CIVIL DA INTERNET)	51
3.4 PROTEÇÃO DE DADOS – LEI N. 13.709/2018 (ALTERADA PELA LEI N. 13.853/2019).....	53
3.5 LEI 13.964/2019 (LEI ANTICRIME).....	54
3.6 LEI 14.132/2021 (CRIME DE PERSEGUIÇÃO).....	55
3.7 LEI Nº 14.155, DE 27 DE MAIO DE 2021(VIOLAÇÃO DE DISPOSITIVO INFORMÁTICO)	56
3.8 PRINCÍPIO DA DIGNIDADE DO USUÁRIO	57
3.9 AUTORIA INFORMÁTICA.....	58
4 CAPÍTULO IV - EXPOSIÇÃO DA INTIMIDADE SEXUAL	60
4.1 EXPOSIÇÃO PORNOGRÁFICA NÃO CONSENTIDA	62
4.2 SEXTORSÃO INFORMÁTICA	65
4.3 STOPNCII.ORG	67
5 CONSIDERAÇÕES FINAIS	69
REFERÊNCIAS BIBLIOGRÁFICAS	71

INTRODUÇÃO

A Revolução Digital vem transformando a realidade da sociedade de modo que está modificando contextos sociais, econômicos e culturais tornando-se impossível não ser correlacionados a virtualidade passando a ser algo necessário na inclusão do cotidiano das pessoas para que possam estar enquadrados no modelo atual de popularização.

Com esse avanço tecnológico dá-se a importância de compreender todo o mecanismo de funcionamento desses instrumentos utilizados na tecnologia com cobertura global incluindo os brasileiros. A taxa de penetração na internet no Brasil ficou em 77,0% da população total no início de 2022. A análise de Kepios indica que os usuários de internet no Brasil aumentaram 5,3 milhões (+3,3%) entre 2021 e 2022.¹

Porém, embora esses meios tecnológicos venham facilitar a vida das pessoas em vários aspectos trazendo agilidade e velocidade nas atividades diárias, também tem seu lado adverso. Os crimes virtuais crescem consideravelmente com rapidez nos quais são revertidas em condutas negativas com incremento da criminalidade no meio digital sem delimitações de fronteiras podendo ocorrer em qualquer lugar.

Por isso a importância de atrair atenção das normas regulamentadoras que devem estar atualizadas conforme a realidade atual com o objetivo de garantir segurança a sociedade no geral. Importante ressaltar que a ocorrência desses crimes embora sejam praticados no mundo virtual, traz consequências voltadas diretamente ao mundo real.

Dessa forma, o presente trabalho tem como objetivo a análise da insuficiência das normas regulamentadoras que se mostra escassa voltadas aos crimes informáticos embora tenha sido revisada ainda não foi o suficiente deixando brechas que são favoráveis aos infratores. A ausência de práticas socioeducativas especificamente voltadas a prevenção de riscos na virtualidade também é um aspecto de importante relevância merecendo uma atenção especial. O trabalho versa sobre os aspectos pertinentes aos crimes virtuais no que tange principalmente sobre a ineficácia e deficiência do Direito Penal Informático.

Para seu desenvolvimento optou-se pela realização de pesquisa bibliográfica, sendo caracterizado como qualitativo e descritivo.

¹ <https://datareportal.com/reports/digital-2022-brazil>

A pesquisa aborda em seu primeiro capítulo uma síntese histórica da internet, elucidando questões desde a sua origem até os dias atuais na sociedade contemporânea. Nesse contexto, faz-se apontamentos da evolução tecnológica e seu papel no contexto social, econômico e cultural dando origem a sociedade digital. Sociedade essa que o Brasil passou a ter acessibilidade de início no meio acadêmico no ano de 1991 e em seguida no ano de 1994 passando a ser acessível para o público em geral. Conforme sua evolução e adequações das redes foram criando fontes de acesso e em destaque na contemporaneidade estão as redes sociais que tem uma potência gigantesca de engajamento com o público virtual, utilizadas como entretenimento e como meio empregatício.

O segundo capítulo são feitos apontamentos sobre os crimes digitais que vem tomando proporção em todos os meios informáticos, criando problemáticas de difíceis soluções pois a falta de preparo para essa onda virtual facilita a entrada de criminosos no sistema ampliando as possibilidades da prática de condutas ilícitas, como também explana a competência para julgar e processar os crimes virtuais comprovando a dificuldade de agir por se tratar de uma rede transnacional, barreiras criadas em matéria de provas dificultando a punição adequada para os delitos praticados prejudicando a dosimetria da pena a ser aplicada.

O terceiro capítulo, por sua vez, estabelece quais leis devem ser aplicadas em respeito ao código vigente acobertadas nas proteções legais como forma de repressão para inibir repetições de práticas delitivas no mundo virtual e consequentemente prevenir novos delitos informáticos. Daí dar-se a comprovação da necessidade de modernização das normas regulamentadoras no ordenamento jurídico brasileiro voltado aos Direito Digital.

No quarto capítulo demonstrou-se a definição dos crimes digitais específicos tais como: Exposição da Intimidade Sexual, Exposição Pornográfica não Consentida, Sextorsão Informática, crimes esses que violam o Direito à Intimidade da vítima como também a Dignidade Sexual.

1 CAPÍTULO I - SÍNTESE HISTÓRICA DA INTERNET

A essência da tecnologia é sua transformação constante desenvolvendo novos meios de dispositivos que passam a ser utilizados com abrangência global.

1.1 INTERNET: DA ORIGEM AOS DIAS ATUAIS

Através da globalização, avanços tecnológicos atingem um público diversificado, de todas as origens, através de ferramentas de grande potencialidade, projetos experimentais viram realidade.

Para Santos (1997, p.108), “A globalização é o processo pelo qual determinada condição ou entidade local consegue estender sua influência a todo o globo e, ao fazê-lo, desenvolve a capacidade de designar como local outra condição social ou entidade rival”.

Diante das necessidades rotineiras para manutenção de controle nos serviços diários, desde os antepassados já existiam formas aplicadas de como organizar as tarefas repetidas. O que atualmente é considerado como informática. Pinheiro (2015, p.89) afirma que “tem-se por definição mais comum que a informática é a ciência que estuda o tratamento automático e racional da informação”.

Para que houvesse a utilização da informática, novas formas de trabalho foram elaboradas, através da criação de novas máquinas, incluindo a origem do computador.

Nos anos 30, essas máquinas começaram a ser construídas com relés eletromagnéticos, porém somente em 1946 estaria finalizado o engenho que claramente se reputaria um passo além das calculadoras. Seu nome era ENIAC - Eletric Numeric Integrator and Calculator, um computador baseado em circuitos eletrônicos. (PINHEIRO, 2015, p.92)

Com os aprimoramentos e os avanços tecnológicos foi possível adaptações positivas para o manuseio dos computadores.

Em 1951 foi lançado o UNIVAC I, o primeiro computador a ser vendido comercialmente. Daí em diante a microeletrônica passa a balizar os avanços na área. O advento do transistor nos anos 60, substituindo a válvula, diminui o tamanho, o consumo de energia e aumenta a potência dos computadores. (PINHEIRO, 2015, p.92)

Com essas inovações vários fatos contribuíram para uma revolução gigantesca com mudanças significativas na realidade social, que cada vez mais passaram a ficar interligadas através de meios digitais. "O primeiro computador com mouse e interface gráfica é lançado pela Xerox, em 1981; já no ano seguinte, a Intel produz o primeiro computador pessoal 286." (PINHEIRO, 2015, p.94)

Em sintonia com o processo inovador de meios de telecomunicações a sociedade passa a inovar as formas de comunicação em busca da eficácia e acesso rápido através do veículo eficiente de repasse de multicomunicação chamado Internet. Sua utilização passou a ser necessária no dia a dia das pessoas, fazendo com que esse sistema evoluísse, tornando -se indispensáveis no cotidiano das pessoas.

Tecnicamente, é possível afirmar que a Internet nada mais é do que um conjunto de protocolos do padrão TCP/IP, que permitem a comunicação entre diferentes computadores. O Conselho Federal Norte Americano da Rede (em inglês: Federal Networking Council – FNC) definiu a Internet como:

Sistema de informações globais que (i) estiver logicamente unido por um endereço único e global, baseado no IP ou extensões subseqüentes; (ii) suportar comunicações TCP/IP (Transmission Control Protocol/Internet Protocol) seguidas ou extensões subseqüentes ou outros protocolos compatíveis ao IP; e (iii) fornecer, usar ou acessar, publica ou privadamente, serviços de alto nível, baseados na comunicação e relacionados à estrutura descrita acima.²

Os Estados Unidos em conflito com a União Soviética protagonizavam a Guerra Fria, nesse momento era necessária uma forma de proteção de suas informações e comunicações, as inovações que tentaram resolver esse problema levaram ao que conhecemos hoje como Internet.

A origem da Internet remonta ao ápice da “guerra fria”, em meados dos anos 60, nos Estados Unidos, e foi pensada, originalmente, para fins militares. Basicamente, tratava-se de um sistema de interligação de redes dos computadores militares norte-americanos, de forma descentralizada. À época, denominava-se “Arpanet”. (PINHEIRO, 2021, p.88)

² Minicursos_SBRC_2009.pdf (ufms.br)

Como meio de defesa e estratégico os militares norte-americanos buscaram um modelo de troca e compartilhamento de informações de forma descentralizada, evitando prejuízo relacionado a percas de informações importantes e possíveis vazamentos de mensagens sigilosas.

A ARPA foi criada com a finalidade específica de realizar pesquisas para que os EUA superassem a União Soviética em tecnologia militar. O projeto da ARPANET teria sido apresentado ao Pentágono como uma forma de rede de comunicação descentralizada que seria capaz de assegurar a integridade dos dados sigilosos até em casos de ataques nucleares. (FIORILLO, 2016, p.12).

Posteriormente, passou a ser usado para fins civis, mais ainda de forma restrita envolvendo apenas em algumas universidades americanas.

"Entretanto, o grande marco dessa tecnologia se deu em 1987, quando foi convencionada a possibilidade de sua utilização para fins comerciais, passando-se a denominar, então, "Internet"." (PINHEIRO, 2021, p.88)

O rápido progresso da tecnologia consegue aumentar de forma impactante a interatividade entre as pessoas e o mundo. A questão é que a internet é uma entidade profundamente democrática seu acesso pode ser feito por qualquer pessoa, facilitando a socialização entre diversos públicos.

No início dos anos oitenta, a ARPANET ainda era uma rede que interligava somente algumas universidades que tinham contratos com a ARPA. Essas universidades, além de desenvolver pesquisas alinhadas com os objetivos militares, necessitavam ter a capacidade financeira para investir em equipamentos e circuitos de comunicação necessários para fazer parte da rede, pois manter um nó da ARPANET custava aproximadamente US\$ 100 mil por ano (HAFNER, 1996, p. 242).

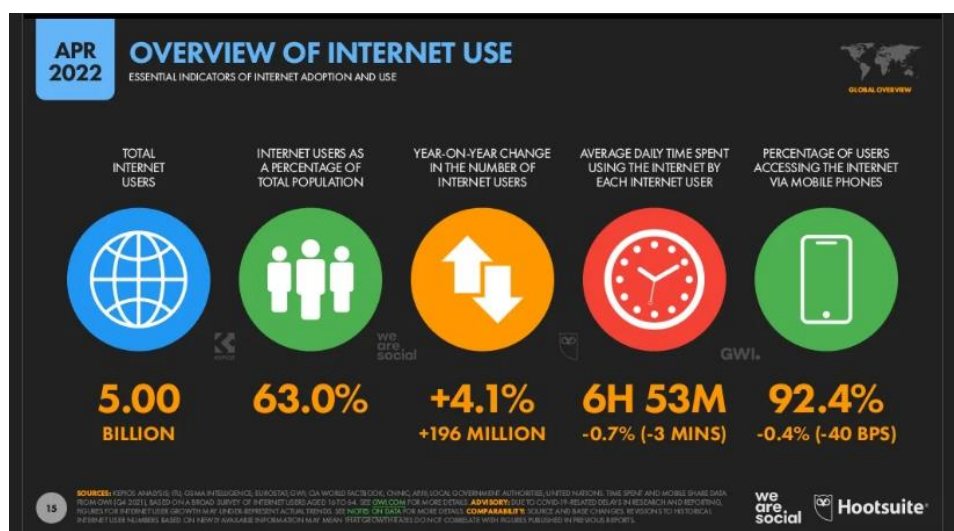
A tal complexidade do sistema foi tomando proporções, que com o passar dos anos foi atingindo diversos países de forma crescente e enriquecedor.

Na década de 90, a Internet passou por um processo de expansão sem precedentes. Seu rápido crescimento deve-se a vários de seus recursos e facilidades de acesso e transmissão, que vão desde o correio eletrônico (e-mail) até o acesso a banco de dados e informações disponíveis na World Wide Web (WWW), seu espaço multimídia. (PINHEIRO, 2015, p.97)

Por trás dos dispositivos utilizados na internet, estão pessoas com objetivos diversificados e que podem utilizar essa capacidade de comunicação para as mais diversas finalidades, atividades essas que se tornam cada vez mais complexas.

O número de usuários ativos está crescendo cada vez mais passando a ter acessibilidade global com um público gigantesco.

Figura 1: Total de Usuários da Internet no Mundo



Fonte: DATAREPORTAL, 2022.

O número de usuários com acesso regular a internet no mundo se aproximou da marca de 5 bilhões de pessoas em janeiro de 2022.

1.2 SOCIEDADE DIGITAL

A convivência em conjunto das pessoas de forma organizada faz com que ações desenvolvidas de maneira consciente venha surgir relações sociais, seguindo um padrão comum de forma coletiva.

Quando um homem age, desloca-se em relação a outros homens: toma uma posição entre os demais, assume uma dimensão no plano social e histórico, e o faz sempre na dependência de suas circunstâncias. Todo fazer humano se refere a homens. Mesmo quando o fazer humano tem como fim a feitura ou a posse de uma coisa, esta é mera condição de uma relação inter-homines. A conduta, portanto, é sempre um fato social e humano, um acontecer no habitat natural do homem, que é a sociedade. (REALE, 2002, p. 386).

A humanidade vive em constantes modificações, proporcionando a interação do homem com a máquina que estão cada vez mais conectados, trazendo inúmeras possibilidades de conexão ampla interligando uma rede de consumidores ávidos por informações, serviços e produtos no meio digital, havendo a inclusão de uma grande massa de pessoas com culturas, costumes e classes sociais divergentes, as relações interpessoais se tornam mais complexas, atingindo até mesmo grupos menos expostos ao vínculo digital. Em busca de meios ágeis e eficazes para ter ações mais imediatas dando origem à sociedade digital.

A sociedade humana vive em constante mudança: mudamos da pedra talhada ao papel, da pena com tinta ao tipógrafo, do código Morse à localização por Global Positioning System (GPS), da carta ao e-mail, do telegrama à videoconferência. Se a velocidade com que as informações circulam hoje cresce cada vez mais, a velocidade com que os meios pelos quais essa informação circula e evolui também é espantosa. (PINHEIRO, 2021, p.70)

As transformações e adaptações envolvidas no avanço da tecnologia de forma integral, atinge de forma direta a sociedade que necessita se moldar para se enquadrar no meio digital, na busca constante de informações que muitas vezes são vistas como esperança de alcance de novos horizontes, tendo em vista que esse universo tecnológico traz diversas oportunidades para o crescimento e desenvolvimento pessoal das pessoas, com a inclusão digital que engloba o mercado do trabalho, educação, social, entre outros.

Novos conceitos passaram a existir com a tecnologia. Enquanto que a maioria dos bens antigamente era representada por átomos, hoje boa parte dela é representada por bits. Os átomos formam a substância tangível, enquanto que os bits compõem a linguagem lógica (intangível) utilizada pela informática para compor os arquivos, programas e sinais de comunicação, representando algo que nos é importante, mas que não existe efetivamente. Consequentemente ao surgimento desse meio ambiente, houve mudanças. O ser humano aumentou seu tempo sozinho, passando a se relacionar e comunicar virtualmente. (SYDOW, 2022, p. 29).

Por outro lado, a tecnologia é tão ampla que acaba perdendo o controle de regularizações e normas que traz como consequência o mau uso dessa ferramenta, devido à falsa impressão de que tudo pode no meio social digital, várias pessoas acabam fazendo o que bem deseja considerando o mundo digital como terra sem lei.

vigente, dessa forma acarreta graves sequelas para quem é atingido por esse ato propagado de forma errônea. A veracidade das informações tem que ser sempre analisada e revista de forma preventiva para que seja evitado tais constrangimentos para os usuários dos meios digitais.

1.3 INTERNET NO BRASIL

A Internet deixou de ser uma rede que acessamos para tornar-se uma rede que nos envolve. Estamos irresistivelmente submergidos em uma cultura do multimídia que modificou definitivamente nossa forma de ver o mundo e analisar os fatos da vida.

Em 1989, a Internet brasileira começa a ser implantada como uma infraestrutura de comunicação para fins acadêmicos, que em seguida começaram a pressionar seu uso de maneira mais ampla.

O primeiro acesso acadêmico à internet no Brasil aconteceu em 1991, de forma cooperativa as instituições custeavam os gastos para ter acessibilidade a essa ferramenta. Em 1994 foram colocados à disposição do público brasileiro em geral, consistia em permitir que o usuário se conectasse por via telefônica.

No Brasil, a utilização da Internet ocorreu inicialmente no meio acadêmico, especificamente na Universidade de São Paulo. No ano de 1988, Oscar Sala, professor da USP, desenvolveu um projeto de interação entre universidades, em âmbito internacional, para que houvesse a troca de informação por meio de uma rede de computadores. Contudo, a autorização da disseminação da Internet para a população, autorizando-se o uso comercial da rede, só foi dado pelos Ministérios das Comunicações e da Ciência e Tecnologia sete anos depois. A incidência direta da Internet nas relações humanas exige a tutela jurisdicional para as informações veiculadas na rede, bem como para as mais diversas relações jurídicas realizadas por meio virtual, mas dotadas de todos os riscos e garantias das relações firmadas no “mundo real. (FIORILLO, 2016, p.16)

Para manutenção do uso da internet era necessário rever os custos que eram altíssimos, houve a implantação de projetos voltados a redução desses gastos de conexão das universidades brasileiras e uma maior distribuição e otimização no uso dos recursos de rede. As redes acadêmicas no Brasil somente convergiram após a estabilização da RNP (Rede Nacional de Pesquisa) e da consolidação do acesso à Internet no Brasil, que por sua vez, precisaram contar não só com a participação do

governo e de empresas privadas, mas também com novos e inesperados aliados advindos da sociedade civil, que forçaram novos rumos para as redes acadêmicas.

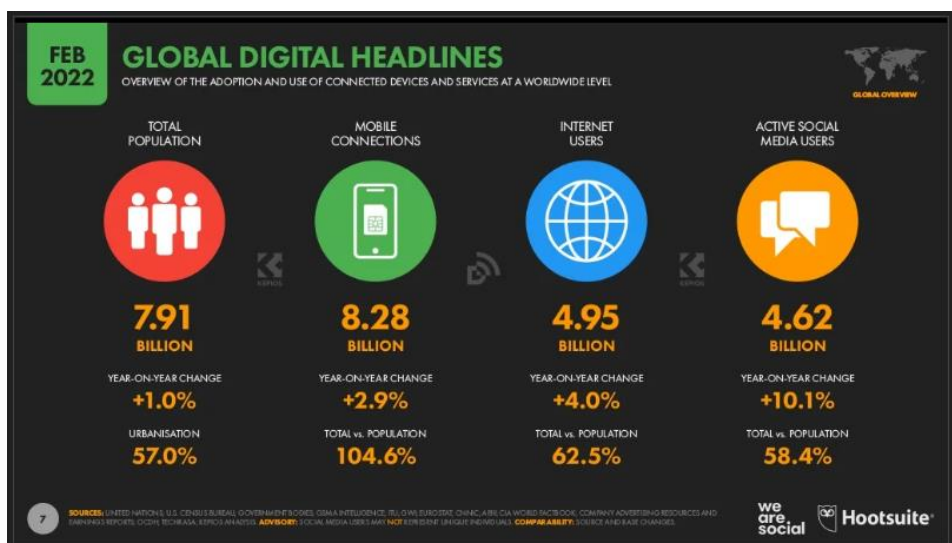
Em alguns países, especialmente nos EUA, surgiam indicadores da extensão do uso da Internet pela comunidade não acadêmica, assim como as primeiras ofertas comerciais dos serviços de provimento de acesso. O que também com o passar do tempo foi tido a abertura comercial da Internet no Brasil.

A exploração comercial da Internet foi iniciada em dezembro/1994 a partir de um projeto piloto da Embratel, onde foram permitidos acesso à Internet inicialmente através de linhas discadas, e posteriormente (abril/1995) através de acessos dedicados via RENPAC ou linhas E1. Em paralelo a isso, a partir de abril/1995 foi iniciada pela RNP um processo para implantação comercial da Internet no Brasil, com uma série de etapas, entre as quais a ampliação do backbone RNP no que se refere a velocidade e número de POP's, a fim de suportar o tráfego comercial de futuras redes conectadas a esses POP's; esse backbone a partir de então passou a se chamar Internet/BR.³

Por se tratar de algo novo, a Embratel deu início ao seu serviço de forma experimental com público restrito, alguns meses após se tornou de modo definitivo, o que passou a ser motivo de conflitos com a iniciativa privada que temia pela a dominação no mercado, mas isso não chegou a acontecer pois a posição do governo deixou claro que os serviços da internet no brasil seria de forma mais abrangente possível , apesar que até os dias atuais existe a exclusão digital , por questões muitas vezes financeiras fazendo que mesmo diante de tantos meios existentes para o possível acesso à tecnologia, vários brasileiros ainda estão desconectados. Mesmo assim o número de usuários cresce de forma avassaladora, tanto em número de usuários quanto de provedores e de serviços prestados através da rede.

³ <https://brasilecola.uol.com.br/informatica/internet-no-brasil.htm>

Figura 2: Total de População Mundial



Fonte: DATAREPORTAL, 2022.

O uso da internet no Brasil vem tomando proporções de inclusão digital aos brasileiros de todas as classes sociais.

Havia 165,3 milhões de internautas no Brasil em janeiro de 2022. A taxa de penetração na internet no Brasil ficou em 77,0% da população total no início de 2022. A análise de Kepios indica que os usuários de internet no Brasil aumentaram 5,3 milhões (+3,3%) entre 2021 e 2022.

Para perspectiva, esses números revelam que 49,37 milhões de pessoas no Brasil não usavam a internet no início de 2022, o que significa que 23,0% da população permaneceu offline no início do ano.⁴

Por ter se tornado uma ferramenta essencial no cotidiano das pessoas estamos propensos à dependência, a proporção de aumento de usuários será cada vez significativos, o que não deixa de ser preocupante de certa forma, pois inclui todos os ramos existentes no meio social, que gera pontos positivos como acessibilidade e crescimento no mundo acadêmico, profissional, meios jurídicos virtuais, interatividade mundial etc.

Porém os pontos negativos também são inclusos, se tornando um modo de distanciamento entre as pessoas pois a internet modifica consideravelmente padrões comportamentais, criando barreiras de comunicação afetiva de forma presencial, deixando o indivíduo vulnerável as redes sociais, é onde entra os riscos associados

⁴ Digital 2022: Brasil — DataReportal – Global Digital Insights

aos crimes digitais. O que vai equilibrar o uso da internet em nossas vidas é o grau de consciência.

Vive-se em um momento de mudanças que possibilita ao homem desenvolver tecnologias inovadoras, com potencial impactante em toda a humanidade.

Figura 3: População Total do Brasil



Fonte: DATAREPORTAL, 2022.

A população total do Brasil foi 214.7 milhões em janeiro de 2022. Uma grande parte dessa população estão ligados na sociedade digital com conexões ativa constantemente.

1.4 REDES SOCIAIS NA INTERNET

A maneira de como a sociedade se agrupa com seus semelhantes vai estabelecendo relações, desenvolvendo afinidades que se mantem e se modifica na esfera social, assim o indivíduo vai delineando e expandindo sua rede conforme a sua realidade.

Uma estrutura em rede – que é uma alternativa à estrutura piramidal – corresponde também ao que seu próprio nome indica: seus integrantes se ligam horizontalmente a todos os demais, diretamente ou através dos que os cercam. O conjunto resultante é como uma malha de múltiplos fios, que pode se espalhar indefinidamente para todos os lados, sem que nenhum dos seus nós possa ser considerado principal ou central, nem representante dos demais. Não há um “chefe”, o que há é uma vontade coletiva de realizar determinado objetivo. (WHITAKER, 1993)

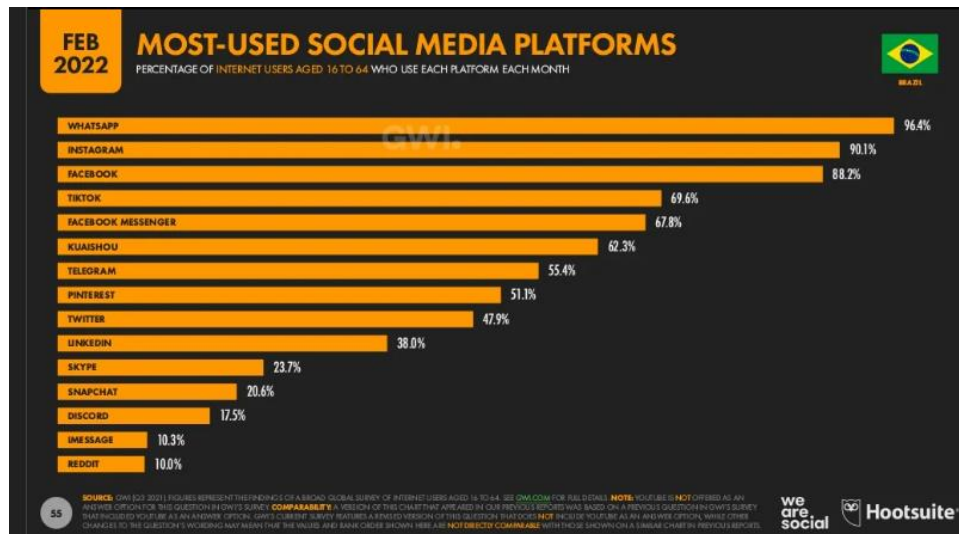
A internet gera uma infinidade de nações virtuais, com interesse variados, desde os primórdios existem grupos sociais, o que hoje podemos definir como redes sociais com objetivo de socializar e se relacionar um com o outro de forma predominantemente descentralizada, com apenas um clique, qualquer pessoa pode acessar uma informação específica e manter contato com pessoas que estão distantes.

As aplicações de relacionamento se consolidam com variedades de meios de comunicação oferecidas no mundo digital, de forma direta e automática. Com o aprimoramento das tecnologias da informação surgiram as redes sociais no âmbito digital. A primeira rede social na Internet surgiu em 1995, nos Estados Unidos e no Canadá.

A sociedade da informática teve sua potência elevada com a popularização das máquinas e suas conexões, bem como a chegada dos smartphones, levando à boa parte da população o acesso a um cotidiano com características próprias, e que tem arquivos e dados intangíveis como mote de sua existência e sustentabilidade. A rede mundial de computadores trouxe velocidade de relacionamentos (comerciais, negociais, humanos, internacionais, etc.) e dissolveu fronteiras físicas, permitindo que o (a) usuário (a)- internauta experimentasse liberdade em grau antes inimaginado. (SYDOW, 2022, p.39.)

Por meio da Internet e das redes sociais temos uma espécie de extensão da personalidade humana, onde os horizontes das comunicações se expandem. Pessoas em diferentes continentes podem se comunicar de forma instantânea, informações são compartilhadas ao piscar de olhos. O crescimento social e cultural com as tecnologias da informação é inovador e espetacular, porém devemos nos atentar ao mau uso dessa ferramenta.

Figura 4: Mídias Sociais no Brasil



Fonte: DATAREPORTAL, 2022.

É de conhecimento que a audiência da mídia tradicional diminui com o passar dos anos por diversos motivos, pois a rede social de certa forma da cobertura necessária para que as pessoas fiquem sempre atualizadas, mas isso não implica que a televisão e a rádio não tenham influências importantes para o desenvolvimento social brasileiro.

A emergência da cultura planetária via redes de teleinformática instalou definitivamente uma crise na hegemonia dos meios de massa e, com ela, o emprego da palavra “mídia” se generalizou para se referir também a todos os processos de comunicação mediados por computador. A partir de uma tal generalização, todos os meios de comunicação, inclusive os de massa, inclusive o livro, inclusive a fala, passaram a ser referidos pela rubrica de “mídia” até o ponto de qualquer meio de comunicação receber hoje a denominação genérica de “mídia” e o conjunto deles, de mídias. (SANTAELLA, 2004, p. 76)

O comportamento das pessoas se molda com o crescimento dessas redes, sendo capaz de se tornar viciante, ao ponto que preferem um encontro virtual, ao invés dos tradicionais encontros presenciais. Ainda mais agora no período da pandemia da Covid –19, esse hábito passou a ser necessário e exigível na população, com impactos gigantescos no cotidiano das pessoas o que afetou vários pontos do financeiro ao psicológico. O lado positivo em momento pandêmico é que houve alternativas de continuidades de atividades desenvolvidas quer antes era presencial, passou a ser também realizadas de forma virtual. Mas a questão é que esse uso

intensivo gerou uma certa compulsividade nas pessoas, por ter encontrado métodos mais cômodos e rápidos, o que o leva a dependência e centralidade do uso da internet. De fato, a sociabilidade digital é necessária à contemporaneidade, contudo a sociabilidade presencial é essencial e sempre prevalecerá.

Havia 171,5 milhões de usuários de redes sociais no Brasil em janeiro de 2022. O número de usuários de redes sociais no Brasil no início de 2022 foi equivalente a 79,9% da população total, mas é importante notar que os usuários de mídia social podem não representar indivíduos únicos (veja nossas notas detalhadas sobre dados para saber o porquê).

A análise de Kepios revela que os usuários de redes sociais no Brasil aumentaram 21 milhões (+14,3%) entre 2021 e 2022.⁵

As redes sociais online permitem executar ações de receber, enviar, criar e responder mensagens e disponibilizam aplicativos usados para seguir e compartilhá-las, para recomendar ou comentar os posts, tudo isso através de meio eletrônico que hoje a acessibilidade está aumentando, pois o uso principalmente de celulares cresceu bastante e sua disponibilidade com valores variados dos mais simples ao mais sofisticado que tem como cobrir a necessidade do público de diversas classes financeiras.

Com o uso crescente das redes sociais, as pessoas se tornam mais vulneráveis aos riscos eminentes que envolve o meio digital, que por muitas vezes as vítimas são leigas ou até mesmo por falta de uma leitura mais minuciosa acaba se deixando levar para as falsas ideologias brilhantes que o mundo digital repassa, dessa forma passa de usuário ao papel de vítima dos crimes digitais.

Para Moraes (2011, p. 139, apud GOMES, 2017, p. 21) “da mesma forma que as redes sociais podem ser usadas para divulgação de conteúdo útil, ela também tem sido usada por criminosos, que induzem os usuários a clicarem em links e efetuar download de malware”.

Portanto, existe a necessidade de melhorar os investimentos em serviços de segurança, criando normas e técnicas buscando assim, garantir a proteção e privacidade dos ativos de informação. Sendo assim, é de grande importância informar, alertar, ensinar e conscientizar usuários, grupos e empresas sobre as situações de riscos que podem afetar a segurança da informação nesses ambientes virtuais.

⁵ Digital 2022: Brasil — DataReportal – Global Digital Insights

2 CAPÍTULO II - CRIME DIGITAL

O Direito reflete a realidade das condutas humanas, que tem como objeto as ações, reações e transformações ocorridas no seio das sociedades.

O Direito tem uma participação expressiva, significativa e necessária na constituição e determinação dos modos de ação social, determinando, desta forma, o esquema de atuação de cada um dentro do jogo de troca social. (BITTAR, 2022, p.150).

A Convivência em agrupamentos sociais exige que haja um equilíbrio de comportamentos para manutenção da ordem social. Com base nos valores culturais existentes em cada território, é possível conviver em harmonia mantendo o respeito entre os cidadãos com o objetivo de uma convivência pacífica, o que faz necessário que existam normas a serem cumpridas com base legal no direito penal.

"O Direito Penal é o rosto do Direito, no qual se manifesta toda a individualidade de um povo, seu pensar e seu sentir, seu coração e suas paixões, sua cultura e sua rudeza. Nele se espelha a sua alma". (LYRA, 1977, p. 37 apud ESTEFAM, 2021, p.38).

A intimidação penal é válida como forma de penalização diante de tantos pensamentos contrários e formas de reações distintas, não é difícil que algo dê errado, é nesse momento que aumenta a probabilidade de composição de conflitos existentes na humanidade, pois é algo que sempre irá acontecer, recorrer ao direito penal é a última cartada do sistema legislativo, impondo sanção penal ao infrator que venha cometer atos ilícitos.

Caso o bem jurídico possa ser protegido de outro modo, deve-se abrir mão da opção legislativa penal, justamente para não banalizar a punição, tornando-a, por vezes, ineficaz, porque não cumprida pelos destinatários da norma e não aplicada pelos órgãos estatais encarregados da segurança pública. Podemos anotar que a vulgarização do direito penal, como norma solucionadora de qualquer conflito, pode levar ao seu descrédito e, conseqüentemente, à ineficiência de seus dispositivos. (NUCCI, 2014, p. 66).

É de suma importância manter o respeito em qualquer circunstância mesmo diante das punições estabelecidas, impedindo ações que não venham violar os direitos de outrem, algo que afeta diretamente a honra do indivíduo, se tornando um ato inconstitucional, violando um dos princípios basilares da Constituição Federal/88.

O princípio da dignidade da pessoa humana deve ser mantido independente da sua condição perante a circunstância dada.

O Princípio da Dignidade da Pessoa Humana, insculpido no art. 1, III, da Constituição Federal se apresenta como um valor de aplicação geral nas áreas do Direito, orientando as atividades estatais, inclusive dos três poderes. No Direito Penal Brasileiro sua interpretação é especialmente vista como uma regra quanto à aplicação da pena e também à duração do processo, quase sempre voltada, assim, para a construção de um axioma de proteção ao acusado ou ao condenado. Porém, não há dúvidas de que sua aplicação não está restrita apenas à investigados, acusados, réus e condenados, devendo ser estendida a todo e qualquer indivíduo, inclusive às vítimas de condutas. (SYDOW, 2022, p. 151).

Diversos fatores fazem com que um indivíduo aja de forma ilícita, o que dificulta identificar o fator determinante para tal atitude, pois envolve vínculos familiares, sociais, financeiros, psicológicos, entre outros, que passa a colaborar na prática do crime, a questão é complexa e vai muito além da simples “vontade” do agente.

Inicialmente, cumpre salientar que o conceito de crime é artificial, ou seja, independe de fatores naturais, constatados por um juízo de percepção sensorial, uma vez que se torna impossível classificar uma conduta, ontologicamente, como criminosa. Em verdade, é a sociedade a criadora inaugural do crime, qualificativo que reserva às condutas ilícitas mais gravosas e merecedoras de maior rigor punitivo. Após, cabe ao legislador transformar esse intento em figura típica, criando a lei que permitirá a aplicação do anseio social aos casos concretos. (NUCCI, 2014, p. 137).

Infração Penal é uma maneira usada para que se possa manter controle nos riscos existentes e dessa forma conseguir o combate ou ao menos amenizar que atos criminosos sejam praticados. A modificação cultural que está sendo inovada na atualidade vem transformando de forma impactante costumes e práticas na sociedade com uma velocidade absurda. Se moldar a esse novo modelo é necessário e preciso, para que possa acompanhar a era tecnológica.

Na Era Digital, o instrumento de poder é a informação, não só recebida, mas refletida. A liberdade individual e a soberania do Estado são hoje medidas pela capacidade de acesso à informação. Em vez de empresas, temos organizações moleculares, baseadas no Indivíduo. A mudança é constante e os avanços tecnológicos afetam diretamente as relações sociais. (PINHEIRO, 2015, p.115)

A realidade é que atualmente se torna quase impossível manter uma rotina longe da virtualidade, as modificações que vem surgindo exige das pessoas a portabilidade de meios digitais o que pode ser chamado de inclusão digital, apesar que ainda existem sim pessoas excluídas desse mundo de tecnologias, porém seu desenvolvimento não será compatível com a exigibilidade de fazer parte da sociedade da informação.

Sendo assim, a sociedade da informação, que vive no mundo físico e no mundo digital, exige que, cada vez mais, seus participantes executem mais tarefas, acessem mais informações, rompendo os limites de fusos horários e distâncias físicas; ações que devem ser executadas num tempo paralelo, ou seja, digital. (PINHEIRO, 2021, p.68)

Com o desenvolvimento da tecnologia e da interação online, se tem a necessidade de se editar normas e regras que regulamentem as relações da nova era digital como forma de impedir, investigar e reprimir condutas lesivas na rede, por se tratar de uma sociedade convergente e diversificada, dessa forma para cumprimento desses regulamentos nasce o Direito Digital.

O Direito Digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas. (PINHEIRO, 2021, p.112)

No meio digital a maior fonte de riqueza é a informação e o conhecimento. Esse avanço tem influência de países desenvolvidos que comporta ferramentas tecnológicas de última geração. Com uma abrangência global é de suma importância a manutenção de um controle mais rígido pois inevitavelmente o fluxo de dados tem um aumento avassalador, o que se fez necessário criar regulamentos a serem cumpridos e respeitados e assim ter maior segurança no mundo virtual.

Tendo como base o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia aplicável desde maio de 2018.

Diversos instrumentos normativos, de fonte nacional e supranacional, procuraram nos últimos anos regular o tratamento de dados pessoais. Entre eles sobressai, na Europa, o Regulamento (UE) 2016/679 do

Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (RGPD), aplicável desde 25 de maio de 2018, o qual foi complementado em Portugal pela Lei n.º 58/2019, de 8 de agosto, que assegura a sua execução na ordem jurídica portuguesa. No Brasil, avulta a este respeito a Lei Geral de Proteção de Dados (LGPD), n.º 13.709, de 14 de agosto de 2018, alterada pela Lei n.º 13.853, de 8 de julho de 2019, a qual deverá entrar em vigor na sua plenitude, em razão do disposto na Lei n.º 14.010, de 10 de junho de 2020, a 1 de agosto de 2021, data a partir da qual passarão a aplicar-se as respetivas normas sancionatórias. (WACHOWICZ, 2020, p. 3).

O uso da tecnologia fornece benefícios e facilidade de interação no meio social, porém gera riscos que devem ser controlados através de regulamentos de forma preventiva, evitando possíveis violações.

Brasil é 5º maior alvo de cibercrimes no mundo.

Brasil já ultrapassou volume de ataques de 2020 apenas neste 1º semestre, com total de 9,1 milhões de ocorrências, considerando apenas os de “ransomware”.⁶

Ransomware é de um meio de resgate fraudulento que consegue realizar o bloqueio do dispositivo e em seguida cobrar pelo desbloqueio sem que a vítima venha descobrir trata-se de um software de extorsão.

Limites são impostos pela lei LGPD (Lei Geral de Proteção de Dados, a Lei n 13.709/18) aprovada em 2018 e entrou em vigor em setembro de 2020 no Brasil. Medidas de segurança são cobradas para garantir os direitos dos proprietários dos dados, com o objetivo de uso adequado para a função específica e com isso evitar danos que vem acarretar violação da segurança dos dados. Os responsáveis por esses danos é o controlador e operador dos dados, que poderão sofrer sanções administrativas conforme as infrações cometidas.

EMENDA CONSTITUCIONAL Nº 115

Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

As Mesas da Câmara dos Deputados e do Senado Federal, nos termos do § 3º do art. 60 da Constituição Federal, promulgam a seguinte Emenda ao texto constitucional:

Art. 1º O caput do art. 5º da Constituição Federal passa a vigorar acrescido do seguinte inciso LXXIX:

⁶ Brasil é 5º maior alvo de cibercrimes no mundo - InfoMoney

Art. 5º. LXXIX – é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.⁷

Deve ser levado em consideração o comportamento dos usuários que cada vez mais vem normalizando a exposição de dados na internet, principalmente nas redes sociais, isso é preocupante pois a falta de cuidados deixa vulnerável o acesso aos dados pessoais gerando risco a privacidade.

Os crimes exclusivamente cibernéticos são aqueles que necessariamente precisam do meio computacional para cometer tal crime (como é o caso do crime de invasão de dispositivo informático, artigos 154-A e 154-B do Código Penal Brasileiro). Já os crimes cibernéticos abertos são aqueles que podem ou não ser praticados pelo dispositivo ou sistema informático, como é o caso de dos crimes de violação de direito do autor ou estelionato, que pode ser praticado tanto no ambiente virtual quanto fora do mesmo. (WENDT; JORGE, 2012, p. 19).

Pois faz parte da estratégia no meio digital em redes, que é ter disponibilidade desses dados para que seja traçado o perfil do usuário e se torne dependente virtual, se mantendo conectado constantemente, pois no mundo real da atualidade para que se possa estar um passo à frente é importante ser atualizado sobre as novas tecnologias.

Por ser mais confortável e mais rápido, o ambiente informático passou a ser mais e mais adotado recebendo mais investimentos, mas confiança e tornando – se parâmetro / padrão. Por conseguinte, passou também a ser um ambiente potencial para lucro e benefícios, tornando – se alvo da delinquência por conta de sua potencialidade, suas vulnerabilidades, erros de programação, falhas de segurança, técnicas de sobrepujamento, engenhosidade social e até mesmo por mero prazer. (SYDOW, 2022, p. 29).

A tecnologia abrange todos os setores, não apenas no computador, mas nos celulares, entre outros, e está intrinsecamente ligada ao desenvolvimento econômico, a informatização impulsiona a maximização dos lucros através das novas ferramentas digitais que tem um alcance gigante de usuários.

O desenvolvimento de cookies fez com que se elevem as estratégias invasivas (algumas delas conhecidas como KYC ou “know your customer ou “conheça seu consumidor “, em tradução livre) em que a

⁷ <https://legis.senado.leg.br/norma/35485358/publicacao/35485850>

navegação memoriza as preferencias do cliente conforme ele navega pelas páginas e informam o fornecedor para que ele melhor direcione suas ofertas. Também, os assistentes virtuais e televisores que “ouvem” o que falamos no dia a dia, interpretam, e nos sugerem serviços e produtos. (SYDOW, 2022, p. 61)

O impacto da evolução no meio digital traz situações que nem sempre é benéfica para os usuários, o mau uso dessa ferramenta pode criar perigo e consequentemente vem as consequências, práticas socialmente desagradáveis e indesejadas passando a se tornar um crime como no mundo real, modificando apenas o ambiente que está sendo praticado que é o virtual.

Contudo, a compreensão dos riscos da sociedade da informação, ainda não está adequadamente inserida na mentalidade da população mundial que permanece utilizando a ferramenta de modo muitas vezes irresponsável, inconsequente e carente de uma educação digital de qualidade que inclua prevenção e lógica e consequencial de ações informáticas. (SYDOW, 2022, p.39).

Por um excesso de confiança o ser humano passa a ser ousado, confiante de que por estar do outro lado da tela, para algumas pessoas ainda é considerada como uma terra sem lei, e hoje a realidade não é bem assim, as ações delituosas são sim consideradas como crime que vem se propagando e se desenvolvendo conforme a globalização dessa nova era digital.

Segundo Jesus: “Para a doutrina internacional, os crimes virtuais tiveram início na década de 1960, quando foram identificadas as primeiras referências sobre o tema, cuja maior parte foi de delitos de alteração, cópia e sabotagem de sistemas computacionais.”⁸

Por ser uma ferramenta de alcance global esses atos irão se proliferando e tomando conhecimento e proporção assustadora, pois se trata de um espaço público, amplo e universal. Existem diversas formas de práticas criminosas e para que seja apontado como crime é necessário que tenha sido praticado por meio ou contra sistemas de informática.

Toda atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, base de ataque ou como meio de crime é conhecido como cibercrime. Outros termos que se referem a

⁸ JESUS, Damásio Evangelista de. Manual de Crimes Informáticos. 1ª ed. São Paulo: Saraiva, 2016, pg. 17

essa atividade são: crime informático, crimes eletrônicos, crime virtual ou crime digital. (CASSANTI, 2014, p. 6).

A realidade é que quanto maior se torna o público de conectados, certamente crescem as descobertas por meio de produção e experiências que contribuem de forma benéfica e também de forma negativa, criando uma nova estrutura social aonde não existem desiguais na anonimidade virtual. Toda essa mudança se torna desafiador para o campo do Direito que é preciso se moldar conforme a atualidade pede, atualizando as novas linguagens, as novas formas de produzir indícios e provas entre outras novidades que surgem com rapidez na tecnologia da informação. Dessa forma é fundamental que a sociedade jurídica evolua juntamente com o avanço tecnológico, pois o delito informático ocorre em toda a virtualidade constantemente.

Os desafios jurídicos do Direito Digital incluem a quebra de paradigmas, a descentralização, a dificuldade em definir limites territoriais e físicos, a velocidade com que as decisões devem ser tomadas e a crescente capacidade de resposta dos Indivíduos. A Internet gera uma infinidade de nações virtuais — pessoas, empresas e instituições de várias partes do mundo unidas por interesses os mais variados.

O grande desafio do Direito é enfrentar essa contradição entre globalização e individualização, que é a grande característica de nossa era — uma era de transição, em que convivem conceitos aparentemente tão díspares. (PINHEIRO, 2021, p.74)

A velocidade das transformações na sociedade digital é uma barreira para o meio jurídico, que não há tempo hábil para criar jurisprudência de forma célere. A construção de novas fontes para lidar com os problemas criminais informáticos é de extrema necessidade, pois a realidade é que as existentes no ordenamento vigente estão aquém do adequado para o segmento atual decorrentes de novas consciências e desenvolvimentos da sociedade.

Primeiro há o surgimento de uma onda de delinquência informática em que milhares de pessoas são vitimizadas e, apenas após isso (e após reportagem em programa de televisão ou após um congressista ser diretamente vitimizado) surge um esforço legislativo tardio, reativo e inútil para fins de evitação de prejuízos e punição pregressa. (SYDOW, 2022, p. 88).

2.1 COMPETENCIA PARA PROCESSAR E JULGAR OS CRIMES VIRTUAIS

Essas condutas delituosas precisam ser investigadas e apreciadas pelo juízo competente, para que seja penalizado de maneira eficaz em cada caso concreto. A complexidade do ambiente informático abrange o mundo inteiro, o que torna a investigação muito mais dificultosa, por se tratar de um território dificilmente demarcável.

“Num universo de magistrados, a competência é conceituada como a medida ou delimitação da jurisdição[...] (TÁVORA, 2013, p.247)”.

Vale ressaltar que a conexão dos usuários da internet é mistificada por diversas culturas que regem as normas elaboradas com a realidade de cada território. Dessa forma surge a problemática da resolução do mérito em questão.

Para melhor esboçar a questão, vamos tomar como referência o Direito Internacional, pelo qual se estabeleceu que, para identificar a norma a ser aplicada, diante da extrapolação dos limites territoriais dos ordenamentos, deve-se averiguar a origem do ato e onde este tem ou teve seus efeitos, para que se possa aplicar o Direito do país que deu origem ou em que ocorreram os efeitos do ato. (PINHEIRO, 2021, p.132)

Porém na internet existe o dilema da dificuldade de detectar o local que o interlocutor está interagindo.

Por trás de uma postagem existe um caminho complexo coberto de várias ações até chegar no objetivo principal, e mesmo que seja possível encontrar o dispositivo utilizado, não descobrir o verdadeiro autor do delito, nada é resolvido pelo fato de não haver a certeza causando a imprecisão de autoria, o que não pode existir em respeito ao princípio do in dubio pro reo.

"Lembre-se, por oportuno, que a defesa não terá de convencer o juiz a ponto de não restar nenhuma dúvida a respeito, pois no processo penal, como regra de julgamento, adota-se o in dubio pro reo." (ESTEFAM, 2022, p.791)

A sociedade digital por ter uma abrangência global, a demarcação do território é uma tarefa desafiadora, o que dificulta na determinação de qual norma deverá ser utilizada, pois a virtualidade elimina a barreira geográfica, criando um ambiente de relacionamento virtual, com mistificações de nacionalidades, culturas e normas a serem aplicadas.

O Direito Penal Informático termina tratando tanto de direito produzido internamente cuja aplicação se dá sobre fatos ocorridos fora do Brasil

(Direito Penal Internacional) quanto em situações de normas internacionais que vigoram dentro do Brasil (Direito Internacional Penal) ; as duas porque a virtualidade , em regra, não é território nacional , mas também não há tratado decretando nem regras especiais nem a internacionalidade desse ambiente, colocando, na realidade , a classificação desse ramo de direito em uma situação característica. (SYDOW, 2022, p. 249)

É uma questão a ser analisada no Direito Informático por seu caráter ilimitado, sem barreiras físicas, tendo em vista que o Direito em seu caráter resolutivo é limitado, terá que aderir novas regulamentações, principalmente quando se trata da territorialidade que tem como objetivo a aplicabilidade da lei no local do cometimento do crime.

De acordo com o art. 5º, caput, do CP, “aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional”. Com tal enunciado, nosso Código acolheu o princípio da territorialidade da lei penal, isto é, a lei penal brasileira aplica-se a todos os fatos ocorridos dentro do nosso território. (ESTEFAM, 2022, p.385)

Mas quando se trata de crimes virtuais essa delimitação se torna uma problemática pois os criminosos não precisam de um território (solo) para efetuar um delito informático, pois o ciberespaço não possui limitações geográficas, implica que se usa a não territorialidade.

A rede digital é transnacional em sua essência, sem fronteiras e descentralizada tornando –se possível seu funcionamento de modo globalizado. O fator positivo é a agilidade e rapidez de repasse informacional de forma eficiente, mantendo todos conectados e atualizados, mas como tudo tem seu ponto negativo, essa abrangência quando se trata de crimes virtuais, por ser um meio ambiente amplo de cobertura mundial isso gera dificuldades jurídicas investigativas e processuais. Com o aperfeiçoamento de prestação de serviço o armazenamento em nuvem também da acessibilidade de dados sem demarcação territorial para usuários de nacionalidades diferentes, o que pode gerar conflitos de normas entre países que tem regras específicas e legislação diversa.

O critério de não territorialidade do delito aplica-se à questão de que há um grande incremento na facilidade com que se alastram golpes, mídias, desinformação prejudicial (fake news) e malwares. Os limites de restrição de fronteiras ou linguagem não se aplicam. Impedir a entrada de um agente delinquente assassino e procurado em um país impede-o de perpetrar delitos. Mas nada impede o ingresso na

virtualidade, que se alastra eficientemente se a linguagem utilizada for convincente e a língua, universal. (SYDOW, 2022, p. 309)

A realidade é que a informática transborda fronteiras geográficas repassando comunicação instantânea, deste modo, ocorre condutas extraterritoriais.

Para ser de Competência Federal terá que haver dano a incolumidade pública e oferta pública, porém, passa a ser de Competência Estadual se for de forma unitária e sem oferta pública, é assim que caminha a jurisprudência. Importante destacarmos que o Brasil ratificou a Convenção de Budapeste (Convenção sobre o Cibercrime) através do Decreto 37/2021.

Em busca de solucionar conflitos de interesse a jurisdição se utiliza da lei cabível em cada caso concreto, como forma punitiva para os que infringem, resguardando a ordem jurídica e a autoridade da lei. As competências jurisdicionais estão fundamentadas no Código de Processo Penal, conforme:

Art. 69. Determinará a competência jurisdicional:

I - o lugar da infração;

II - o domicílio ou residência do réu;

III - a natureza da infração;

IV - a distribuição;

V - a conexão ou continência;

VI - a prevenção;

VII - a prerrogativa de função.⁹

A rapidez que a tecnologia vai inovando é necessário que o ordenamento jurídico passe a se adaptar e se molde conforme suas necessidades para que não haja um crime sem uma lei anterior que o defina, em respeito à luz do princípio da legalidade.

O Princípio da Legalidade ou da reserva legal é outro desdobramento de suma importância no Direito Penal Informático. Por ele, apenas a lei federal pode criar fundamentação para criminalização de condutas. Os famigerados usos e costumes não tem condão nem de gerar reprovabilidade penal, nem de afastar a tipificação de uma prática. (SYDOW, 2022, p. 89)

Embora que no cotidiano práticas delituosas como por exemplo, baixar conteúdo protegidos por direitos autorais, compartilhamento de imagens íntimas se

⁹ http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm

repetam frequentemente, entre outros delitos, não autoriza que costume habitual das pessoas retire sua ilegalidade, apesar que uma grande parte se adeque virando rotina tais delitos, no entanto, é dever de respeitar os princípios que servem para regular as relações da vida , dirigindo condutas e comportamentos na sociedade , juntamente estão as normas que existem para manter a ordem social.

2.2 PROVAS

A prova é o ato que busca comprovar a verdade dos fatos, afim de instruir o julgador.

O autor Lopes Jr. (2017, p. 344) informa que “o processo penal e a prova integram os modos de construção do convencimento do julgador que influenciará na sua convicção e legitimará a sentença”.

Coletar e preservar evidências é fundamental para a apuração dos fatos e responsabilização dos culpados. Para tanto, não é suficiente ter apenas conhecimento técnico. É necessário entender a conduta, os processos, os aspectos jurídicos de atuação e comportamento para realização de um bom trabalho de elucidação de crimes cibernéticos. Além de conhecimento técnico é necessário equipamentos de qualidade para que seja utilizado no processo investigativo em busca de informações relevantes para cada caso ocorrido, e que as investigações sejam céleres no intuito de preservação de vestígios para ser analisados com eficácia.

A prova judiciária tem o objetivo claramente definido: a reconstrução dos fatos investigados no processo, buscando a maior coincidência possível com a realidade histórica, isto é, com a verdade dos fatos, tal como efetivamente ocorrido no espaço e no tempo. A tarefa, portanto, é das mais difíceis, quando não impossível: a reconstrução da verdade. (PACELLI, 2017, p. 174)

Com a obscuridade da rede, a acessibilidade de provas tem suas dificuldades por questões que muitas vezes são destruídas sem deixar rastros, isso faz com que os agentes desse tipo de crime virtual se tornem anônimos. Embora haja mecanismos como forma de detecção do usuário presumidas por um número IP, nomes, senhas, biometria, entre outros, mesmo assim não traz a verdade absoluta de quem está por trás do aparelho utilizado na prática do delito ilícito.

Existem várias formas de camuflagem de identidade que favorece para a não descoberta do usuário de fato gerando incertezas, dentre essas formas estão a omissão do IP, navegar através de navegadores criptografados como o TOR e afins, nuvens criptografadas, e-mails e assim sucessivamente. Inclusive o próprio Direito traz essa cobertura à anonimidade virtual sugerindo métodos criptográficos anonimizadores.

Não vemos nenhum benefício na manutenção do anonimato, que de certa forma pode diminuir a credibilidade das informações veiculadas pela internet, o que já ocorre em alguma medida em vista da falta de fidedignidade da fonte em certas situações. No fundo, o anonimato apenas favorece aqueles que se utilizam da internet para fins escusos. (TEIXEIRA, 2020, p.181)

Como forma resolutiva para descobrir os infratores na rede virtual é preciso um sistema de identificação adequado, como também uma revisão legislativa na responsabilização dos provedores para que venham investir em mecanismos de proteção como fonte de segurança para seus usuários.

A criminalidade do ciberespaço deve ser combatida com as mesmas armas, ou seja, desfrutando das ferramentas oferecidas pelo próprio ambiente informático na prevenção, investigação, prova e repressão dos crimes virtuais. Para isso, fazem-se necessárias unidades policiais especializadas nestes crimes, assegurando a manutenção da integridade das provas/vestígios ao mesmo tempo em que possibilitaria a adequação dos órgãos policiais à velocidade dos crimes digitais. (JORGE, 2012, p. 21)

Uma ferramenta de grande eficácia é a computação forense que visa obter informações por meio da análise de dados de um computador ou sistema através de técnicas especiais que consegue rastrear possíveis riscos virtuais.

Embora não esteja prevista na legislação processual brasileira uma hierarquia de provas, acaba existindo uma prevalência da prova pericial no conjunto probante. Tal preferência decorre do fato de a prova pericial ser produzida a partir de fundamentação científica, não dependendo de interpretações subjetivas. Nenhuma tecnologia, desde o advento do DNA, teve um efeito potencial tão grande em tipos específicos de investigações como a computação forense. (PINHEIRO, 2021, p.486)

Para conseguir acesso de dados que irão contribuir nas investigações é fundamental o respeito ao devido processo legal e devem agir no limite da legalidade. O que cabe apenas o magistrado o poder de ordenar o fornecimento de registros de conexão, função privativa da magistratura. Conforme o artigo 23 do Marco Civil da Internet:

Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro.¹⁰

A cada publicação exposta na rede digital a probabilidade de viralizar é enorme, e isso propaga conhecimento com cobertura global de armazenagem duradoura. Acontece que nem sempre é feliz o repasse de publicações causando constrangimentos para o autor da publicação, gerando conflitos sociais e pessoais afetando diretamente sua vida.

"No Brasil, o direito ao esquecimento foi tratado pelo Enunciado 531 da VI Jornada de Direito Civil do Conselho da Justiça Federal, e coloca que "a tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento". (PINHEIRO, 2021, p.911)

Esse direito se dá através de uma decisão judicial que se dá através de notificação de remoção aos conteúdos ofensivos, o proprietário da postagem pleiteia que a informação seja apagada dos registros, porém não se dá de forma instantânea. Outra situação mais agravante é quando a exposição da intimidade sem autorização causando sofrimento e transtorno psicológico com danos graves, neste caso sendo notificado a rede a remoção deve ser imediata, uma tarefa dificultosa tendo em vista que após postado o conteúdo, sua expansão de acesso pode ser de todos os lugares do mundo de forma instantânea com diferentes políticas de privacidade.

No Brasil, o STJ já decidiu acerca do direito ao esquecimento, cujos precedentes, embora não sejam exatamente sobre o assunto no campo da internet, são muito relevantes. No REsp 1.335.153/RJ (DJe 10-9-2013), o tribunal entendeu que os familiares não tinham o direito de exigir que o crime contra "Aida Curi", ocorrido em 1958, voltasse a ser ventilado por determinado programa televisivo. Já no REsp 1.334.097/RJ (DJe 10-9-2013), tratando do caso que ficou conhecido com a "Chacina da Candelária", o tribunal reconheceu o direito ao esquecimento do autor, uma vez que foi absolvido da acusação do

¹⁰ L12965 (planalto.gov.br)

crime ocorrido treze anos antes da exposição do documentário em programa de televisão. (TEIXEIRA, 2020, p.171)

Os usuários também devem manter a cautela da leitura dos termos de uso e realizar a observação da durabilidade temporal de acesso. Os provedores devem ser transparentes quanto a essas informações, porém os próprios usuários por muitas vezes não têm o cuidado de compartilhamento de informações, dados esses que tem um vínculo objetivo com a pessoa sobrepondo a várias circunstâncias.

2.3 PUNIBILIDADE

Na medida em quem o agente ativo comete um ato ilícito, dar-se ao Estado a possibilidade de puni-lo como forma repressora, afim de corrigir e reduzir repetições de tais condutas reprováveis no objetivo de controle e manipulação comportamentais da sociedade com isso manter a ordem legal e social. O poder punitivo do Estado afigura-se tímido nas diversas questões ligadas à segurança digital, à proteção dos direitos de privacidade, informação, tutela aos bens jurídicos afetados pela delinquência cibernética.

Se o efeito [da punição] fosse simplesmente o inverso do efeito do reforço, grande parte do comportamento poderia ser facilmente explicada; entretanto, quando o comportamento é punido, vários estímulos gerados pelo comportamento ou pela ocasião são condicionados no padrão respondente e o comportamento punido é então deslocado por [displaced by] comportamento incompatível condicionado como fuga ou esquiva. Uma pessoa punida continua 'inclinada' a comportar-se da forma punível, mas ela evita a punição fazendo alguma outra coisa, (Skinner, 1974/1976, p. 69).

Dessa forma para manter a organização da sociedade é fundamental haver regras que devem ser seguidas conforme sua finalidade que é a harmonia de convívio entre as pessoas tanto de forma física, como também no meio virtual. O que de fato na realidade nem sempre é possível tendo em vista por ser tratar de pessoas com variações comportamentais e caráter distintos, a forma de agir consequentemente será diferente uma das outras, o que os leva a caminhos controversos e infelizmente a lugares de um final infeliz.

As necessidades de paz, ordem e bem comum levam a sociedade à criação de um organismo responsável pela instrumentalização e regência desses valores. Ao Direito é conferida esta importante missão. A sua faixa ontológica localiza-se no mundo da cultura, pois representa elaboração humana. O Direito não corresponde às necessidades individuais, mas a uma carência da coletividade. A sua existência exige uma equação social. Só se tem direito relativamente a alguém. O homem que vive fora da sociedade vive fora do império das leis. O homem só, não possui direitos nem deveres. (NADER, 2014, p. 52)

As pessoas acreditam que o ciberespaço é um espaço livre, em que se pode cometer crimes sem ser punido, isso traz insegurança para as vítimas realizar as denúncias e acarreta temor para essas pessoas que sofrem esse tipo de crime, para os infratores resta a impunidade do delito. A vítima (agente passivo) é a peça chave para coleta de elementos indiciários, preservação desses elementos e demonstração de autoria, sem a sua colaboração dificulta bastante no processo, criando barreiras que impede aplicar sanções cabíveis para o infrator gerando ineficácia da lei.

Em decorrência do princípio da legalidade ou da anterioridade da lei penal, a insuficiência ou a ausência de norma penal tipificando os crimes digitais limita a função punitiva estatal, uma vez que influencia na sensação de insegurança e impunidade, com repercussão negativa para a sociedade brasileira e, em especial, para a comunidade internacional, que há mais de uma década vem chamando a atenção para a necessidade e urgência de controle e prevenção de condutas delituosas no ciberespaço. (KUNRATH, 2014, p.61)

A inclusão digital é necessária desde cedo para que não venham ficar de fora na atualidade de forma regressa na era digital, isso implica que a educação digital seja primordial para que os jovens saibam os riscos que estão acometidos na rede virtual e saibam realizar boas práticas digitais com ética e respeito. Mas para que esse público venha ter segurança de acesso virtual é de grande valia o controle parental que controla e restringe conteúdos impróprios para os menores de 18 anos, já que se trata de um usuário hiper vulnerável. Eis a questão sobre a punibilidade, pois é cabível informar que atualmente esses jovens são por muitas vezes mais aptos de manuseio nos aparelhos eletrônicos com habilidades melhores do que pessoas com idade mais avançada, por estar em convívio com a tecnologia desde muito cedo, dessa forma existe grandes possibilidades que delitos são de autoria dessa juventude.

Não se deve confundir a inimizabilidade com a impunidade. Conforme os artigos apontam, há regras no Estatuto da Criança e do Adolescente (Lei n 8.069/90) para apuração e processo de atos infracionais, além de responsabilidade civil decorrente de seus atos, recaindo sobre seus responsáveis. (SYDOW, 2022, p. 382)

Importante rever os deveres e cuidados dos responsáveis desse ciberdelinquentes jovens de uma forma socioeducativa no uso das redes virtuais. A prevenção é uma iniciativa afim de evitar delitos que venham gerar consequências negativas.

2.4 PRINCÍPIO DA RESPONSABILIDADE PENAL SUBJETIVA E RESPONSABILIDADE DA PESSOA JURÍDICA

No Brasil como também em outros países o homem sozinho ou com participação coletiva é que pode ser considerado sujeito ativo do crime. Através de sua conduta indo ao contrário com o Direito de forma ilícita não basta apenas o nexo causal é preciso existir a vontade consciente da realização do ato ilícito (dolo) ou ao menos uma culpabilidade. É considerado inadmissível a responsabilidade penal objetiva pela ausência de dolo ou culpa.

Via de regra, apenas indivíduos são sujeitos a responsabilização penal e apenas quando e se for demonstrado o elemento subjetivo, que só é identificado em pessoas físicas. Não se admite no Brasil, em tese, a responsabilidade objetiva, por conta do Princípio da culpabilidade que exige a presença do elemento subjetivo no tipo. (SYDOW, 2022, p. 94)

Diante do que foi exposto fica claro que não há responsabilização criminal da pessoa jurídica. O que na verdade está incoerente com a realidade, já que os provedores tem participação ativa nos serviços digitais, com condutas que liga diretamente na prática de um delito informático.

O Marco Civil afastou completamente a responsabilidade civil dos provedores de conexão, no tocante ao conteúdo que trafega por eles, chegando ao ponto de proibir expressamente que estes realizem qualquer tipo de monitoramento sob o argumento de se estar ferindo a liberdade e a privacidade dos usuários. (PINHEIRO, 2021, p.243)

Se tratando em matéria penal informática a não demonstração da culpa ou dolo exclui a responsabilização dos provedores de acesso, serviços e conteúdos por serem pessoas jurídicas.

2.5 PRINCIPIO DO NE BIS IN EADEM

Da a garantia da não repetição de punição pelo mesmo fato, sendo assim após o cumprimento da pena volta seu status quo ante na sociedade, tendo em vista que o objetivo do Direito Criminal é a repreensão para que não venha ter repetições dos delitos.

Mas se tratando de delitos informáticos para que se tenha um resultado, sempre ocorre mais de uma prática ilícita violando um bem jurídico, mas que em respeito ao princípio supracitado acaba ficando impune, já que o foco é no resultado final do agente.

Consunção ou absorção é o fenômeno jurídico pelo qual uma sucessão de condutas que possua um elo de dependência ou objetivo único apenas gerará uma única consequência jurídico-punitiva. Também apresentada pela ideia de que o delito – fim absorve o delito-meio, isto aponta que por vezes condutas diversas podem ser unificadas. (SYDOW, 2022, p.105)

2.6 PENAS

O Direito Penal impõe regulamentações que devem ser obrigatoriamente observadas por todos. O Estado reprime condutas que lesionam os direitos dos cidadãos, como forma punitiva atribui sanções aos infratores cuja finalidade é a repressão ao crime perpetrado e a prevenção de novos delitos.

O objetivo da pena, fundamentalmente, é reeducar a pessoa humana que, cedo ou tarde, voltará ao convívio social, de modo que a progressão é indicada para essa recuperação, dando ao preso perspectiva e esperança. Deve o merecimento ser apurado no caso concreto, contando, em alguns casos, com a avaliação da Comissão Técnica de Classificação (composta pelo diretor do presídio, dois chefes de serviço, um psiquiatra, um psicólogo e um assistente social), conhecedora do processo de individualização da execução penal (arts. 5.º a 9.º, LEP). (NUCCI, 2020, p.533)

As penas são classificadas em diferentes espécies que são Pena Privativa de Liberdade que acomete a reclusão, detenção e prisão simples, tem a Pena Restritiva de Direitos que tem limitações e tem a Pena Pecuniária que é a multa.

DAS ESPÉCIES DE PENA

Art. 32 - As penas são: (Redação dada pela Lei nº 7.209, de 11.7.1984)

- I - privativas de liberdade;
- II - restritivas de direitos;
- III - de multa.¹¹

Ao observar as penas citadas tem como base voltadas para uma sociedade material, o que na época seria compreensível, já que não tinham ciência de quanto a virtualidade passaria a ter uma tamanha proporção como está na atualidade.

O cometimento da infração penal nem sempre é solitária, é bastante comum de participação cooperativa na prática da conduta delitiva, pode se dar por meio da coautoria, concurso de delinquentes ou de agentes, entre outras formas, o que classifica concurso de pessoas denominados plurissubjetivos.

A escolha legislativa brasileira para o trato com o tema autoria foi a adoção da teoria restritiva, diferenciando autoria e participação a partir do uso das expressões participação impunível e participação de menor importância. Assim, caberá ao magistrado a verificação do grau de participação de cada elemento participante da conduta delitiva. (SYDOW, 2022, p.396)

O concurso de delitos no mundo virtual é um caso a ser analisado, diante que um só conduta alcança um público imenso, capaz de gerar vários resultados na sociedade, se tratando de delitos de alastramento rápido.

De acordo com o delito praticado existe sua gravidade no quanto de pena que ele acarreta, a natureza do crime traz consigo sua reprovabilidade gerando a dimensão do agravamento. A prevenção é o eixo para evitar os delitos criminais, acontece que mesmo trabalhando a forma educativa na sociedade sempre tem práticas que infringem o ordenamento jurídico restando a reparação do dano e reeducação dos infratores, para conseguir ressocializar na sociedade.

A pena é usada no sentido de comprovar que o cometimento de ato ilícito trará punição, com objetivo de intimidar e evitar sequencias de atos delituosos que tem

¹¹ DEL2848compilado (planalto.gov.br)

poder de afetar diretamente a privação de direitos, inclusive direito fundamental como a liberdade, isso impacta a vida das pessoas que passa por tal situação e até mesmo os que tem ligação direta com os as vítimas. Mas ao mesmo tempo se torna preocupante quando se fala em liberdade quando usada com excesso potencializando as práticas ilícitas que estão aumentando com aperfeiçoamento de métodos de execução.

Provavelmente, punir um usuário que pratica delito informático com uma pena de prestação pecuniária, restituição do prejuízo gerado e também um cerceamento de acesso à virtualidade por um período longo colocaria o agente em uma situação de dificuldades suficientes para desestimular uma repetição. (SYDOW, 2022, p. 414)

Retirar o direito de acesso a virtualidade seria um castigo e tanto, tendo em vista que a dependência que as pessoas estão de se manter conectadas, está se equiparando a um direito fundamental, pois afeta diretamente as facilidades que o mundo virtual proporciona, sendo revogadas é uma punição severa e eficiente pela tamanha importância que se tem hoje no cotidiano das pessoas o uso de ferramentas digitais.

“É de extrema importância questionar-se o modo de responsabilizar criminalmente os delinquentes informáticos e como aplicar penas, ao invés de simplesmente aceitar que grande parte dos ilícitos seja de pequeno potencial ofensivo”. (SYDOW, 2022, p. 417)

A rigidez das penas deve ser relativa conforme a atualidade e a realidade da sociedade, sendo assim o Direito Penal necessariamente deve acompanhar o mesmo ritmo do avanço tecnológico e ser posto em prática com excelência.

3 CAPÍTULO III - ESTRUTURAS LEGAIS NO ÂMBITO DIGITAL

A sociedade é construída por diversas culturas, costumes, religiões , condições econômicas e pensamentos políticos diferentes, isso faz com que ocorra acordos e desacordos na convivência das pessoas gerando divergências de condutas, assim para que haja um controle de convívio social em harmonia e organizada de acordo com nível de desenvolvimento da sociedade, foi necessário criar regulamentos com objetivo de impor regras e normas que devem ser respeitadas, nas quais dita o que é certo ou errado e o que o indivíduo pode ou não fazer , desenvolvidas pelo poder legislativo.

Compete ao Sistema Legislativo fazer o filtro de todas as valorações e expectativas de comportamento da sociedade, mediante processos decisórios, para que elas possam adquirir validade jurídica. A capacidade da norma de refletir a realidade social determina o grau de eficácia jurídica de um ordenamento. Eficaz é aquilo que é capaz de efetivamente produzir efeitos, ou seja, o conceito de eficácia envolve aceitação e obediência. (PINHEIRO, 2021, p.78)

Na sociedade o risco está presente de forma direta que devem ser vistos com cautela através de ferramentas preventivas traçando parâmetros normativos. O Direito é responsável pelo equilíbrio comportamental da sociedade através de normas com capacidade de interpretar a realidade social, gerando segurança no sentido que existem meios de penalidades de forma adequada a solução ao caso concreto e que venha ter eficácia de poder coercitivo penalizando os infratores responsáveis.

O Princípio da Legalidade ou da reserva legal é outro desdobramento de suma importância no Direito Penal Informático. Por ele, apenas a lei federal pode criar fundamentação para criminalização de condutas. Os famigerados usos e costumes não tem condão nem de gerar reprovabilidade penal, nem de afastar a tipificação de uma prática. (SYDOW, 2022, p. 89)

O Direito Penal Informático é um ramo que está em processo de formulação, as legislações ainda estão sendo analisadas e carecem de tecnicismo elaborados com função de adaptação ao avanço tecnológico que traz consigo novas modalidades de delitos.

Apesar de chamarmos os crimes de tal natureza de “nova modalidade de delito” a primeira legislação sobre o tema provém dos Estados Unidos da América do Norte, data de 1984 e foi denominada de Computer Fraud and Abuse Act (CFAA) seguida em 1986 da Electronic Communications Privacy Act (ECPA). (SYDOW, 2022, p.315)

Abordar sobre o Direito Penal na Informática é uma tarefa que merece atenção, pois de fato não tem como de forma imediata a legislação ser alterada, assim surgem barreiras que impede o alcance legislativo com o avanço tecnológico.

“O Brasil inicia sua história legislativa no Direito Penal informático de modo relativo no ano de 1997 com a promulgação da Lei n 9.459/1997”. (SYDOW, 2022, p. 258)

A problemática está na velocidade que a tecnologia vai inovando que acarreta dificuldade do sistema jurídico em incorporá-la. “Em seguida, há o verdadeiro e próprio início do Direito Penal Informático com a promulgação da Lei Federal n 9.983/2000, original da PL n 933/1999”. (SYDOW, 2022, p. 259)

A morosidade causada pela não aplicação desses preceitos acarreta consequências muitas vezes irreversíveis, mesmo assim não é aceitável que o legislador aguarde os delitos nocivos se agravarem gerando prejuízos graves na sociedade para apenas então legislar.

A única forma pela qual poder-se-ia diminuir o prejuízo à população seria um monitoramento ativo por parte dos legisladores, no sentido de identificar como a ciência e as academias vêm identificando e escrevendo sobre as tendências da criminalidade informática e chamar especialistas para contribuir apresentando a problemática e apoiando na própria redação legislativa. (SYDOW, 2022, p. 89)

Apesar de alguns especialistas acreditarem que a preocupação com dados pessoais surgiu nos Estados Unidos anos 60, a primeira lei oficialmente direcionada ao tema foi criada em Hessen, na Alemanha, na década de 70.

Nesse período, o avanço da computação e da indústria nos países mais desenvolvidos teria impulsionado o estado alemão a criar normas para regular a privacidade no país. Essa também seria a primeira vez que o conceito de proteção de dados seria introduzido no cenário jurídico da Alemanha.

Embora o conceito tenha sido desenvolvido desde o início da década de 70, a legislação só foi finalizada e implementada em 1978. Neste mesmo ano, países como

França, Noruega, Suécia e Áustria também criaram suas próprias leis sobre como as informações de seus cidadãos poderiam ser utilizadas e exportadas.

Em 1981, uma convenção elaborada pelos países membros do então Conselho da Europa ajudou a unificar e desenvolver melhor as normas para o tratamento automatizado de dados pessoais.¹²

No Brasil o avanço tecnológico trouxe necessidades de proteção digital com o objetivo de minimizar os riscos de violação aos direitos individuais e coletivos.

Na própria Constituição Federal de 1988 já se tem uma visão protetiva relacionado a garantia de direitos fundamentais.

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (Vide Lei nº 9.296, de 1996)¹³

Alterações forma realizadas com abrangência da inclusão dos meios digitais, conforme a Emenda Constitucional N 115.

EMENDA CONSTITUCIONAL Nº 115

Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

As Mesas da Câmara dos Deputados e do Senado Federal, nos termos do § 3º do art. 60 da Constituição Federal, promulgam a seguinte Emenda ao texto constitucional:

Art. 1º O caput do art. 5º da Constituição Federal passa a vigorar acrescido do seguinte inciso LXXIX:

“Art. 5º LXXIX – é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.” (NR)

Art. 2º O caput do art. 21 da Constituição Federal passa a vigorar acrescido do seguinte inciso XXVI:

“Art. 21 XXVI – organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei.” (NR)

Art. 3º O caput do art. 22 da Constituição Federal passa a vigorar acrescido do seguinte inciso XXX:

“Art. 22 XXX – proteção e tratamento de dados pessoais.”¹⁴

¹² <https://assisemendes.com.br/historico-protecao-de-dados/>

¹³ http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

¹⁴ <https://legis.senado.leg.br/norma/35485358/publicacao/35485850>

3.1 O DIREITO DO CONSUMIDOR NA ERA DIGITAL

O Código do Consumidor entrou em vigor no Brasil em 1991, com o objetivo de proteção aos mais vulneráveis na relação de consumo. Desde a antiguidade já existia regulamentação do comércio.

“Consoante a lei 235 do Código de Hamurabi, o construtor de barcos estava obrigado a refazê-lo em caso de defeito estrutural, dentro do prazo de até um ano (...)” (SANTOS, 1987.p. 78)

Conforme vai evoluindo a tecnologia, as ferramentas comerciais digitais também vão se aperfeiçoando acompanhando o crescimento do consumo eletrônico. O e-commerce brasileiro está se expandindo cada vez mais, pois a sociedade digital está cada vez mais em busca de flexibilidades que preenche suas necessidades e rapidez em suas compras, o que é um risco, pois se torna vulnerável ao modelo que esse tipo comercial digital traz, pois, a intervenção humana é mínima no ato da compra e o preenchimento de dados para a finalização da compra fornecem dados que podem ser utilizados para definição de perfis que influencia os consumidores passando a comprar frequentemente, esse é o objetivo das empresas que trabalham com anúncios personalizados.

Na era digital surgem novos direitos como a Lei do E-commerce (Decreto nº 7.962/2013), que regulamentou o CDC sobre a contratação no comércio eletrônico. Art. 1º Este Decreto regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico, abrangendo os seguintes aspectos:

- I - informações claras a respeito do produto, serviço e do fornecedor;
- II - atendimento facilitado ao consumidor; e
- III - respeito ao direito de arrependimento.¹⁵

Adaptações foram feitas para os consumidores digitais, tendo como base o Direito do Consumidor de forma física, com proteção pelo Código de Defesa do Consumidor na Lei do E-commerce e no Decreto nº 10.271/2020.

Quanto às relações firmadas entre partes sediadas em países diversos, aplicam-se a Lei de Introdução às Normas do Direito Brasileiro – LINDB (antiga Lei de Introdução ao Código Civil – LICC) e, no que couber, o Decreto Legislativo n. 538/2012, o qual aprovou o

¹⁵ http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm

texto da Convenção de Viena sobre Contratos de Compra e Venda Internacional de Mercadorias. (TEIXEIRA, 2015, p.47)

3.2 LEI 12.737/12 (LEI CAROLINA DIECKMANN)

Diante de uma situação específica que aconteceu com a atriz Carolina Dieckmann que teve arquivos copiados de seu computador pessoal, foi proposto o projeto de lei PL 2793/2011 transformado na LEI 12.737/12 "Lei Carolina Dieckmann" entrando em vigor no dia 02 de abril de 2013.

Esta lei está voltada para crimes virtuais e delitos informáticos, tipificando os crimes cibernéticos, com foco na invasão de dispositivos sem a permissão do proprietário.

Os delitos previstos na Lei Carolina Dieckmann são:

. Invasão de dispositivo informático

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

Ação penal

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.”

. Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública

Art. 266..

§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.

. Falsificação de documento particular

Art. 298. Falsificação de cartão

Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.¹⁶

Diante da elevação do número de crimes praticados com o uso de dispositivos eletrônicos reformas foram necessárias no Direito Penal, como forma não apenas de punir, como também de desestimular a prática de novos delitos.

3.3 LEI N. 12.965/2014 (MARCO CIVIL DA INTERNET)

Lei regulamentadora do uso da internet no Brasil que estabelece princípios, garantias, direitos e deveres atribuídos aos usuários, empresas e governos na web sejam cumpridos.

Foi promulgada a Lei n. 12.965, em 23 de abril de 2014, a qual é chamada de Marco Civil da Internet (MCI). Trata-se de uma lei principiológica, pois estabelece parâmetros gerais acerca de princípios, garantias, direitos e deveres para o uso da internet no Brasil, além de determinar algumas diretrizes a serem seguidas pelo Poder Público sobre o assunto (Lei n. 12.965/2014 – Marco Civil da Internet – MCI, art. 1º). Em seu texto também há regras específicas a serem cumpridas por agentes que operam na internet, especialmente as dirigidas aos provedores de acesso e de conteúdo. (TEIXEIRA, 2015, p.155)

Suas regras e princípios têm implicação direta em tudo o que ocorre na internet em âmbito brasileiro. Está lei tem pilares que é de suma importância para o direito digital, um deles é a garantia à liberdade de expressão.

Quanto à liberdade de expressão (cujo direito está assegurado na Constituição Federal, art. 5º, IX, consistindo na liberdade de

¹⁶ L12737 (planalto.gov.br)

manifestação intelectual, artística, científica e de comunicação, sem censura ou necessidade de licença), o usuário da internet pode se expressar escrevendo e postando o que bem entender, sendo que o conteúdo somente pode ser removido pelo provedor mediante ordem judicial. (TEIXEIRA, 2015, p.157)

Importante frisar a parte desfavorável que pode trazer efeitos colaterais, a expressão de liberdade se for utilizada de maneira exacerbada na intenção de expor conteúdos digitais ofensivos, a utilização de perfis falsos, é uma situação de cuidado especial, tendo em vista que na virtualidade a amplitude e as ferramentas tecnológicas tem a camuflagem de autoria que dificulta a identificação se utilizando do anonimato, fazendo com que aumente as violações que são contempladas com a impunidade.

O texto final que foi promulgado está bem claro quanto à garantia de liberdade de expressão, todavia, deveria ter sido tratada melhor a questão da vedação ao anonimato prevista pela Constituição Federal de 1988. Infelizmente, o anonimato associado à impunidade faz aumentar a agressividade e a violência entre as pessoas dentro da Internet, especialmente no que diz respeito aos crimes contra a honra." (PINHEIRO, 2021, p.158)

Dentre as mudanças ocorridas no Direito Penal Informático, é importante abordar sobre a Lei n 13.718/2018 que versa sobre crimes contra a dignidade sexual.

É recorrente diversos casos que acontece no Brasil e com a tipificação do crime se torna mais preciso a punição aos que cometem esse tipo de essa prática libinosa.

Esta lei deu início ao delito específico, apresentando -o da seguinte forma:

Artigo 218- C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor a venda, distribuir, publicar ou divulgar, por qualquer meio de comunicação de massa ou sistema de informática ou telemática -, (...) sem o consentimento da vítima, cena de sexo, nudez ou pornografia. Em seguida vem a Lei n 13.772/2018, que trouxe para o ordenamento jurídico penal informático o delito de registro não autorizado da intimidade sexual.

Em 26 de setembro de 2019 (publicado em 01 de outubro de 2019), é publicada a portaria n 93 da Presidência da República / gabinete de segurança Institucional que aprovou o Glossário de Segurança da Informação, com importante caráter complementar – interpretativo.

Em 24 de dezembro de 2019 a Lei n 13.968 acrescenta, dentre outras coisas, o parágrafo 2 ao artigo do Código Penal triplicando o montante de pena para situações em que os delitos contra a honra são cometidos ou divulgados em quaisquer modalidades de redes sociais da rede mundial de computadores.

Aos 26 de dezembro de 2019, entra em vigor a Lei 13.968 que, insere no parágrafo 4 no artigo 122 do Código Penal criando uma

qualificando para delito de induzimento, instigação ou auxílio a suicídio ou automutilação, permitindo que a pena seja até dobrada se a conduta for realizada por meio da rede de computadores, de rede social ou transmitida em tempo real. (SYDOW, 2022, p. 261-262)

3.4 PROTEÇÃO DE DADOS – LEI N. 13.709/2018 (ALTERADA PELA LEI N. 13.853/2019)

Os dados pessoais é um conjunto de informações utilizados para identificação de pessoas. Dados esses que são muito utilizados nos serviços digitais, através de preenchimento de formulários que por muitas vezes são abusivos exigindo dados além do que preciso.

A disciplina da proteção de dados pessoais emerge no âmbito da sociedade de informação, como uma possibilidade de tutelar a personalidade do indivíduo, contra os potenciais riscos a serem causados pelo tratamento de dados pessoais. A sua função não é a de proteger os dados per se, mas a pessoa que é titular desses dados. (MENDES, 2014, p. 27)

Na observância de casos verificados com o uso de dados na rede digital percebeu a necessidade da aplicação do ordenamento jurídico na criação de regulamentos com base de parâmetros estabelecidos mundialmente tratando de direitos para os tutelares dos dados com controle e proteção para coibir condutas ilegais e passar confiança para a sociedade.

A discussão acerca da necessidade de haver uma tutela jurídica para os dados e a privacidade das pessoas iniciou na década de 1970 na Europa, que culminou implicando na Diretiva n. 95/46/CE, que por sua vez foi substituída pelo Regulamento n. 2016/679166 (GDPR – General Data Protection Regulation; em português, Regulamento Geral de Proteção de Dados), o qual entrou em vigor em 2018. Essa norma europeia datada de 2016 passou a ter forte influência na aprovação de normas de proteção de dados pelo mundo, especialmente no Brasil. Sendo assim, a partir de 14 de agosto de 2018 foi incorporada ao ordenamento jurídico brasileiro a Lei n. 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD). Inicialmente a lei brasileira tinha uma *vacatio legis* (tempo para entrar em vigor uma lei) de 18 meses, mas, com as alterações promovidas pela Lei n. 13.853/2019 (lei que cria a ANPD – Autoridade Nacional de Proteção de Dados), o prazo de início da vigência da LGPD foi ampliado para 2 anos, igualando assim a lei europeia. Dessa forma, seu primeiro dia de vigência é 16 de agosto de 2020. (TEIXEIRA, 2020, p.234)

O objetivo principal dessa lei foi manter a maior transparência com os titulares de dados pessoais com a finalidade de legítima de forma adequada e conforme a necessidade sem uso excessivo que venha passar do limite de uso dos dados, que venha ser de livre acesso aos titulares de forma segura prevenindo riscos que possam surgir e que possa ser protegido com responsabilidade.

"Frise-se que o titular de um dado é a "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento" (LGPD, art. 5º, inc. V). Pessoas jurídicas de quaisquer espécies não são titulares de dados pessoais para efeitos da LGPD – Lei n. 13.709/2018." (TEIXEIRA, 2020, p.236)

As sanções administrativas para o descumprimento da LGPD são de competência exclusiva da ANPD a sua aplicação. Conforme o artigo:

Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública.
Parágrafo único. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação.¹⁷

A lei deve proteger o usuário e manter o controle de prevenção para que não ocorra condutas ilegais, com fornecimento de dados obtidos em excesso e não fugir da finalidade principal do sistema ou serviço.

3.5 LEI 13.964/2019 (LEI ANTICRIME)

Com intuito de combate ao crime organizado foi necessário a realização de reformas na legislação penal e processo penal no Brasil. Com amplo crescimento de crimes no ambiente virtual, vetada foi o § 2º do art. 141 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, alterado pelo art. 2º do projeto de lei.

Art. 141

§ 1º

~~§ 2º (VETADO). (NR)~~

¹⁷ L13853 (planalto.gov.br)

§ 2º Se o crime é cometido ou divulgado em quaisquer modalidades das redes sociais da rede mundial de computadores, aplica-se em triplo a pena.’ (NR)”¹⁸

3.6 LEI 14. 132/2021 (CRIME DE PERSEGUIÇÃO)

A sociedade digital tem poder de engajamentos que está aumentando a cada segundo que comporta tribos com opiniões e posicionamentos divergentes. A conexão interligada na vida pessoal com a vida digital transparece o cotidiano dos internautas e isso gera uma certa intimidade com os seus seguidores. Comunidades são formadas virando uma família virtual. Porém como na vida real nem sempre são flores no convívio familiar, é nesse momento que entra os conflitos e discussões que invade o íntimo de cada ser através de comportamentos agressivos e opiniões contrárias, que gera perseguições e invasão de privacidade tornando –se uma ação ilegal denominando –se o famoso Stalking (perseguição insistente). A prática prevê condenações para quem comete o crime em qualquer meio, seja digital ou físico. Conforme previsto:

Art. 147-A. Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade.

Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa.

§ 1º A pena é aumentada de metade se o crime é cometido:

I – contra criança, adolescente ou idoso;

II – contra mulher por razões da condição de sexo feminino, nos termos do § 2º-A do art. 121 deste Código;

III – mediante concurso de 2 (duas) ou mais pessoas ou com o emprego de arma.

§ 2º As penas deste artigo são aplicáveis sem prejuízo das correspondentes à violência.

§ 3º Somente se procede mediante representação.¹⁹

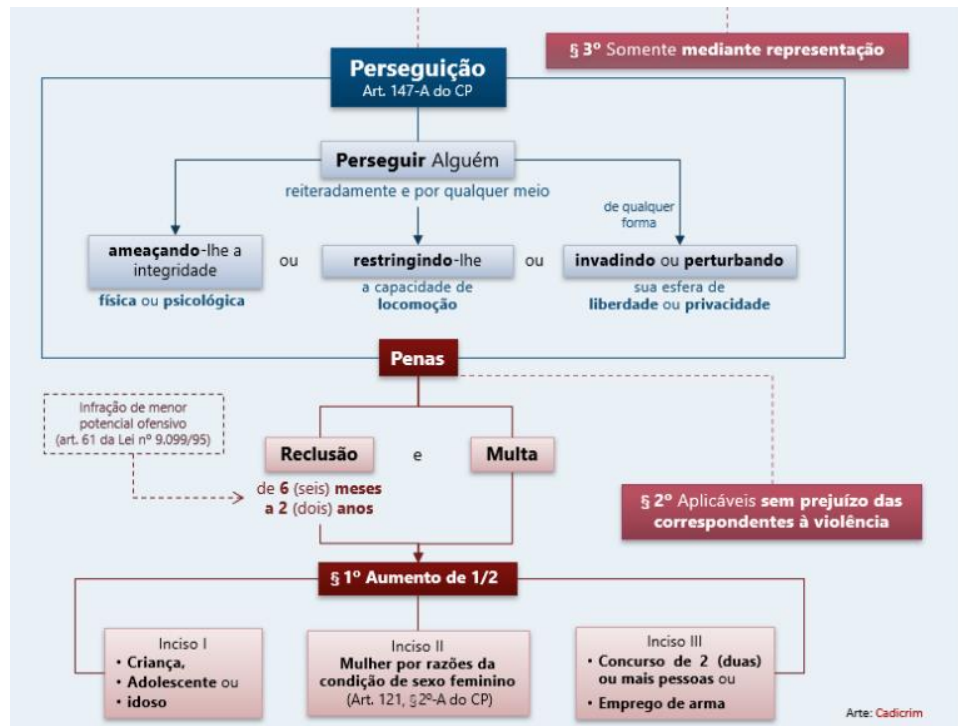
O objetivo desta lei é proteger a liberdade individual que é um direito constitucional e que deve ser respeitado não permitindo a sua violação através de

¹⁸ L13964 (planalto.gov.br)

¹⁹ L14132 (planalto.gov.br)

condutas constrangedoras invadindo severamente a privacidade prejudicando a vida das pessoas que sofrem com esse tipo de crime que consiste em perseguir alguém conforme está informado na gravura abaixo:

Figura 5: Perseguição Art. 147-A do CP



Fonte: CADICRIM, 2021.

Formas de perseguição e as penas dadas para prática do delito.

3.7 LEI Nº 14.155, DE 27 DE MAIO DE 2021(VIOLAÇÃO DE DISPOSITIVO INFORMÁTICO)

A prática delitiva de invasão de dispositivos é uma conduta realizada com frequência feita da seguinte forma, o agente faz uso inapropriado do dispositivo sem a permissão do proprietário de forma invasiva para auferir vantagem indevida, passando a ser considerado crime em razão do acréscimo do artigo 154-A ao Código Penal.

O delito previsto no art. 154-A, caput, do Código Penal consiste em invadir dispositivo informático alheio, conectado ou não a rede de computadores, por meio da violação indevida de mecanismo de segurança e com o objetivo de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do

dispositivo ou instalar vulnerabilidade para obter vantagem ilícita. (TEIXEIRA, 2020, p.1142)

Independente se o dispositivo está com acesso à internet, pois o que é analisado é o dolo o criminoso age de forma consciente com intuito prejudicial o crime se configura na invasão não autorizada, que dependendo do prejuízo causado poderá ter elevação da pena.

Havendo prejuízo de ordem econômica à vítima, a pena será aumentada de um sexto a um terço, conforme o § 2º.

Se em razão da invasão ocorrer o controle remoto não autorizado do dispositivo invadido – ou mesmo a obtenção de conteúdo de comunicações eletrônicas privadas (como os e-mails), informações sigilosas, segredos comerciais ou industriais –, a pena passa a ser de reclusão, e não de detenção. Nestas hipóteses, aumenta-se a pena se houver divulgação, comercialização ou transmissão a terceiro, de forma gratuita ou não, dos dados ou informações obtidas, nos termos dos §§ 3º e 4º do art. 154-A do Código Penal. (TEIXEIRA, 2020, p.1144)

A reversão da pena de detenção por reclusão deve ser reavaliada quanto o local que esses criminosos irão ficar reclusos levando em consideração que se for alocado com os demais prisioneiros de crimes comuns sem relação a virtualidade, irão criar vínculo e trocas de debate tendencioso a proliferação de infratores aptos para realizar crimes virtuais gerando uma máfia virtual.

3.8 PRINCÍPIO DA DIGNIDADE DO USUÁRIO

A revolução que o mundo virtual vem trazendo na sociedade é um acontecimento irreversível, pois muito dificilmente as pessoas irão se desfazer da tecnologia, as exigências no mundo real não permitem mais que isso aconteça. Isso pede que o equilíbrio seja mantido nas relações sociais englobando o lado físico e virtual que andam conectados no cotidiano das pessoas. É preciso ter um olhar de cuidado nesse vínculo de vivência e para manter a harmonia nas redes é necessário manter o respeito aos direitos dado de forma civilizada e pacífica. Para a eficácia dessa ordem é necessário a participação do Estado, juntamente com os provedores e os próprios usuários que também passem a ter mais cautela monitorando e preservando seus dados, já que as empresas provedoras não estão dispostas em

investir em sistema de proteção pois isso tem um custo alto que não serão gastos até que se torne obrigatoriedade.

É preciso cuidado ao interpretar que tais valores da virtualidade compreendem exatamente os mesmos valores da vida real. Não compreendem. Valores informáticos expressam-se de modo diferente na rede e, por isso, merecem proteção e principiologia específicos. (SYDOW, 2022, p. 153)

O não respeito a privacidade dos usuários, realizando a exposição de seus dados, como também de sua intimidade já que se trata de pessoas por mais que estejam por trás de uma tela, tem sua vida, seus sentimentos, sua família, seu emprego, tudo isso pode ser afetado de forma direta ou indiretamente podendo gerar desconfortos e prejuízos incomensuráveis.

3.9 AUTORIA INFORMÁTICA

A comprovação da autoria é uma dificuldade existente tornando-se um desafio para autoridades responsáveis na descoberta do infrator, a identidade não pode ser detectada apenas por logs e IPs, pois não estão necessariamente associados a uma pessoa. Sendo assim, o princípio *in dubio pro reo* (na dúvida em favor do réu) tem que ser respeitado.

Trazido na Constituição Federal de 1988, mais precisamente no artigo 5º, inciso LVII que *in verbis* se tem que “ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória”. (BRASIL, 1988, p. 292)

No meio informático delimitar possíveis autores não é uma tarefa simples, pois a tecnologia é impessoal, e os limites numéricos não existem relacionado a restrição de suspeitos.

Há diversos métodos de mascaramento de identidade virtual. Há possibilidade de uso de embaralhadores de IP (IP scramblers, uma das espécies de ID cloakers ou camuflagem de identidade) - que têm como finalidade modificar constantemente a identidade do computador de onde se origina o acesso -, há a possibilidade de uso de sites de anonimidade que se utilizam de mecanismo de criptografia por camadas (onion protocol), o uso de provedores em países sem normativos reguladores da Internet, entre tantas outras técnicas. (SYDOW, 2022, p. 329)

A sensação que os infratores têm de proteção , faz com que se tornem destemidos pelo fato de acharem que não estão sendo observados, tornando-se cada vez mais ousados nas práticas delitivas no mundo virtual, tendo em vista que esses infratores são cientes da morosidade do sistema judiciário e o despreparo de equipamentos de segurança e até mesmo na falta de preparo policial para os crimes virtuais e a fragilidade da população ,que não são aptos a detectar um possível risco de ser vítima na rede digital por não compreender o funcionamento de táticas para realização dos delitos. Embora que para os usuários mais atentos por ter mais conhecimento na área digital, chega a ter a intuição de previsibilidade de ser alvo.

A melhor definição de vítima advém da resolução n 40/34 de 29.11.85, da Assembleia Geral das Nações Unidas, que aponta internacionalmente a definição de vítima como sendo:
Pessoa que, individual ou coletivamente, tenha sofrido danos, inclusive lesões físicas ou mentais, sofrimento emocional, perda financeira ou diminuição substancial de seus direitos fundamentais, como consequências de ações ou omissões que violem a legislação penal vigente, nos Estados – Membros, incluída a que prescreve o abuso de poder. (SYDOW, 2022, p.773-774)

A necessidade de se manter conectado chega a extasiar as pessoas e dessa forma não passam a ter noção da probabilidade altíssima de se tornar vítima de um delito informático.

4 CAPÍTULO IV - EXPOSIÇÃO DA INTIMIDADE SEXUAL

Não raro os relatos de casos que expõe imagens de pessoas nos meios virtuais, que muitas vezes acarreta sérias consequências na vida da vítima desse delito. Antes de 2018 não existia tipo penal que pudesse recorrer para punir os responsáveis dessa prática delituosa o que resultava em impunidade. Conforme foi aumentando os casos e verificando a gravidade da realidade na sociedade, percebeu a necessidade da criação do tipo penal denominado de “Exposição de Intimidade Sexual”.

A inovação legislativa com alteração no artigo 216 inserindo uma letra B e a criação do capítulo I-A com título e subtítulo do Código Penal busca coibir a exposição não autorizada da intimidade sexual. Trata-se da Lei n 13.772/18.

A lei de autoria do Deputado João Arruda – portanto é lei de origem da Câmara dos Deputados – e trata-se de evolução do PLC n 18 de 2017, substitutivo ao PLC n 5.555/13 (com 5 proposições apensadas). Originalmente, tratava-se de projeto de lei com a finalidade de criminalizar a pornografia de vingança ou vingança pornográfica. Tanto é assim que tanto a justificativa do projeto de Lei quanto o Parecer SF n 146 de 2017 146 de 2017. (SYDOW, 2022, p. 492)

Formulado esse artigo com intuito de reprovação de forma punitiva para casos de registros de materiais de natureza erótica ou pornográfica referidos a cena de nudez ou ato sexual ou libinoso de caráter íntimo e privado.

O novel artigo 216-B tem a seguinte redação: Produzir, fotografar, filmar ou registrar, por qualquer meio, conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado sem autorização dos participantes.

Pena - detenção, de 6 (seis) meses a 1 (um) ano, e multa.

Parágrafo único. Na mesma pena incorre quem realiza montagem em fotografia, vídeo, áudio ou qualquer outro registro com o fim de incluir pessoa em cena de nudez ou ato sexual ou libidinoso de caráter íntimo. (SYDOW, 2022, p. 494-495)

Devido o ato delituoso abordado no artigo supracitado a vítima passa por constrangimentos, visto que a possibilidade de ser consumado o delito já traz um peso que acarreta o lado pessoal da vítima incluindo o social, familiar, até mesmo o lado profissional, tudo isso leva a vítima se tornar vulnerável. Pensando nisso que o Direito Penal agiu de forma coercitiva para que a sociedade venha se conscientizar que na atualidade haverá punição para esse tipo de conduta delituosa.

“Quanto ao bem jurídico atingido, as figuras do caput e do parágrafo único são IMPURAS. Isso porque o bem jurídico atingido é exclusivamente a dignidade sexual violada em situação de captação ou montagem”. (SYDOW, 2022, p. 510)

É de suma importância abordar sobre as crianças e adolescentes que também enfrentam esse tipo de abuso sexual, por aproveitamento de sua vulnerabilidade os infratores fazem proveito dessa facilidade que tem no meio virtual de comunicação entre adultos e menores, pela falta de fiscalização ativa que impeça essa ligação, sendo assim, facilita a prática de comportamentos abusivos e criminosos. Dada a sua imaturidade precisam ser cuidadas e respeitadas.

Com o avanço da tecnologia digital e sua utilização por crianças e adolescentes, com mais frequência os detentores do poder familiar precisam estar atentos e zelar pela privacidade e a exposição da imagem da prole nesse ambiente. Sob o pretexto de assegurar o direito à participação e à expressão infantojuvenil, a integridade moral dos filhos muitas vezes é ameaçada ou violada quando há excesso dessa exposição. (MACIEL, 2022, p.553)

É incontestável a participação no mundo virtual das crianças e adolescentes, inclusive com acesso a conteúdo adultos, o uso imoderado da tecnologia gera graves sequelas físicas e psicológicas, isso deve levar bastante consideração para cuidados e fiscalização permanente que deve partir do próprio vínculo familiar. Ações educativas devem ser elaboradas como meio de prevenção e proteção aos vulneráveis e com o objetivo de demonstrar a dosagem certa na utilização dessas ferramentas tecnológicas.

A proteção à imagem da criança e adolescente tem previsão na Constituição Federal de 1988, com cobertura da Lei federal 8.069/90 - ECA (Estatuto da Criança e Adolescente) tendo como direito fundamental.

Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente: (Redação dada pela Lei nº 11.829, de 2008)²⁰

O sharenting (prática de compartilhamento da vida pessoal da criança) pode ter efeitos negativos, devido a exposição virtual pode se tornar um atrativo de curiosidade para os criminosos.

²⁰ L8069 (planalto.gov.br)

4.1 EXPOSIÇÃO PORNOGRAFICA NÃO CONSENTIDA

O comportamento humano por diversas vezes os leva a uma situação indesejada e cruel e uma dessas condutas é o fenômeno contemporâneo classificada como divulgação não consentida de imagens íntimas. A normalidade hoje em dia de tratar o mundo virtual como algo comum faz com que a sociedade não venha a temer o quanto essa ferramenta é poderosa e seu poder pode ser usado de forma favorável para alguns, como também tem reações adversas para outras, tudo depende de como é feita sua utilização e de quais cuidados são tomados em seu uso. Conforme evolui a tecnologia os usuários vão se aperfeiçoando e se moldando com novas descobertas. A facilidade com que os meios digitais têm para liberação de conteúdos pornográficos contribui para que ocorra a popularização da pornografia.

No aspecto legal criminal, a conduta de exposição pornográfica não consentida foi tipificada pela Lei 13.718/2018, que inseriu no Código Penal o artigo 218-C, com a seguinte redação:

Art. 218-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia.

A pena é de reclusão de um a cinco anos, se o fato não constitui crime mais grave. (SYDOW; CASTRO, 2022, p. 178)

A medida em que vai surgindo novos delitos na rede virtual, também avança as buscas para inibir tais condutas que não se trata apenas de uma exposição em si, ultrapassa a intimidade interior, acarretando danos para o lado exterior que é o meio social de vivência das vítimas que na maioria das vezes são grupos vulneráveis como mulheres e crianças e adolescentes que inúmeras vezes se calam por vergonha de julgamentos de familiares e da sociedade, o que acaba deixando impune os responsabilizados.

Dados da Organização Não Governamental (ONG) brasileira SaferNet - importante instituição de promoção dos Direitos Humanos na Internet e da segurança digital - revelaram aumento de mais de 20% nas denúncias de discriminação contra mulheres, com mais de 660 registros em um mês. Para os casos específicos de exposição de imagem íntima, o aumento foi de mais de 150%, com mais de 130

registros em um mês, dos quais a grande maioria das vítimas é mulher (PATROCINIO, 2022, p. 18 apud RAMOS, 2020).

Independente da proporção que foi a exposição sendo parcial ou total, ambas representam violação aos direitos de intimidade, de privacidade e da dignidade sexual, isso implica que é cabível um parâmetro indenizatório, como também a análise de programas voltadas a proteção e prevenção que venham inibir esses atos.

A *Revenge Porn Helpline*, operada pela SWGfL, tem o prazer de anunciar o lançamento de StopNCII.org. Trabalhamos em estreita colaboração com a Meta para desenvolver uma nova plataforma para proteger pessoas ameaçadas com o compartilhamento de imagens íntimas sem consentimento. Essa colaboração entre a *Revenge Porn Helpline*, SWGfL e Meta irá para proteger e apoiar aqueles que são impactados por abusos de imagem íntimas em todo o mundo. StopNCII.org representa uma mudança significativa na abordagem da indústria tecnológica. Pela primeira vez, qualquer pessoa afetada por ameaças de compartilhar suas imagens íntimas terá os meios para se proteger em suas próprias mãos, tirando o controle dos criminosos. O compartilhamento de uma imagem íntima sem consentimento pode deixar a vítima vulnerável e impotente. Com essa nova plataforma, as vítimas podem tomar medidas de proteção para garantir que o que se pretendia ser privado, permaneça privado.²¹

A produção material da exposição pornográfica não consentida na virtualidade tem análises a serem vistas no caso da origem que pode ser através da própria vítima, mas não implica o consentimento mesmo realizando a produção de conteúdo, pois infringe inclusive seus direitos autorais.

Outro ponto importante é sobre a autocolocação da vítima que cede sua imagem ao parceiro, mas não significa que se dar o direito de explanação para o público, o que gera um enorme problema quando isso acontece, pois para a viralizar é questões de segundos, já em compensação a demora na identificação de um ataque e descoberta de autoria, gera um prejuízo imensurável para a vítima. “A vítima manipulada para entrar em sítios, ceder informações, clicar em links e fazer downloads suspeitos, termina por gerar sua própria vitimização”. (SYDOW, 2022, p.334)

²¹ StopNCII.org lançou | Linha de ajuda por pornografia de vingança (revengepornhelpline.org.uk)

Quando a divulgação acontece através de terceiros que nada venha a ter relação com a vítima, pessoas essas que tiveram acesso a equipamentos, também é um exemplo de origem de exposição não consentida.

Com relação a posse desse material existem formas diferenciadas de como foi gerada, a consentida na qual a vítima concorda com a elaboração das imagens, filmagens, entre outros, de forma espontânea, não consiste em permissão de divulgação.

Já quando não consentida de fato o material exposto foi conseguido através de invasões de dispositivos espíões, câmeras ocultas, ou seja, meios ilícitos que pessoas com más intenções buscam e realizam os delitos informáticos.

Da mesma forma é a disseminação que pode ser consentida, parcialmente consentida e não consentida, através de motivações que varia conforma cada caso, pode ser por vingança conhecido como (revenge porn), pode ser também para expor o outro com intuito de humilhar ou acarretar prejuízos no meio social afetando o vínculo empregatício, e vários outros motivos como vaidade ou fama do divulgador, chantagem em trocas de recompensas, lucros etc.

Não se pode perder de vista que o consentimento é contextual e deve ser interpretado de forma restrita. Ou seja, o consentimento que um indivíduo dá para alguém de sua confiança captar ou receber uma imagem sua com conteúdo íntimo não se estende, como regra, para que a pessoa possa compartilhar com terceiras essas imagens. O consentimento para questões existenciais tem finalidade específica e se encontra diretamente ligado aos vínculos e relacionamentos estabelecidos. Representa uma das bases legais para o tratamento de dados pessoais e assegura controle ao indivíduo acerca de suas informações. Por estarem em jogo direitos da personalidade, poderá o titular desses direitos livremente e a qualquer momento revogar o consentimento dado, bem como alterar sua abrangência. (TEFFÉ, 2019, p. p4-95)

É perceptível a vulnerabilidade do gênero feminino nos casos da exposição pornográfica não consentida, porém não se trata de exclusividade, pois tendem também a repercussão negativa na comunidade LGBTQIA+. A famigerada percepção de uma sociedade preconceituosa leva a conclusões equivocadas que traz uma visão de erro, não natural, envolvendo a comunidade citada acima, preconceito esse que afeta todo o grupo social.

A correlação da imagem da comunidade LGBTQIA+ com a promiscuidade. A ideia da intensa alternatividade de parceiros, da inconsistência em relacionamentos

estáveis, da preferência por práticas sexuais grupais, de risco ou tabus está fortemente vinculada no imaginário popular a esse grupo. (SYDOW; CASTRO, 2022, p.118)

Se faz necessário promover e implementar políticas de proteção e repressão aos atos discriminatórios, assegurando soluções para os problemas surgidos que afetam a sociedade, com olhar especial para os grupos mais vulneráveis já mencionados nesse trabalho.

4.2 SEXTORSÃO INFORMÁTICA

Com a popularização de diferentes meios eletrônicos com funções riquíssimas de resoluções de imagens com qualidade estimula as pessoas a fazerem o uso dessas ferramentas, até mesmo como forma de elevação de autoestima atualmente com o auxílio dos filtros a inibição das pessoas de se expor diminuiu bastante. Habitualmente já é rotina na sociedade a troca de mensagens pelos aplicativos que pela praticidade e velocidade se torna mais atrativo e interessante para seus usuários.

“A sextorsão encontra na era tecnológica um imenso propulsor da coerção psicológica, que beneficia os autores e apavora as vítimas, uma vez que o potencial de difusão e de danos à intimidade é incalculável”. (SYDOW, 2022, p. 608)

Diante de tantas novidades surgidas na virtualidade, vem inovando as formas de comunicação nessas redes, umas dessas inovações é a prática do sexting (ato de compartilhar conteúdos eróticos em aplicativos de mensagens e em redes sociais).

Na falsa segurança que as pessoas têm, a confiança é uma das bases para que venham a ter coragem de realizar a prática do sexting, dessa forma é uma abertura que se dá para se tornar uma possível vítima da sextorsão informática.

Uma imagem ou sequência íntima ou comprometedor em vídeo pode se converter em um pesadelo se chega a mãos inadequadas. Quando quem a possui submete a pessoa que a protagoniza a chantagem sob a ameaça de que mostrará a alguém ou a tornará pública, estamos diante de um caso de sextorsão [...]. (FERNANDEZ, 2013, p. 84).

Não há uma lei penal específica que puna essa modalidade de forma adequada, fazendo com que os casos sejam analisados conforme o entendimento dos juízes. O que configura a sextorsão é a chantagem que o infrator utiliza através de

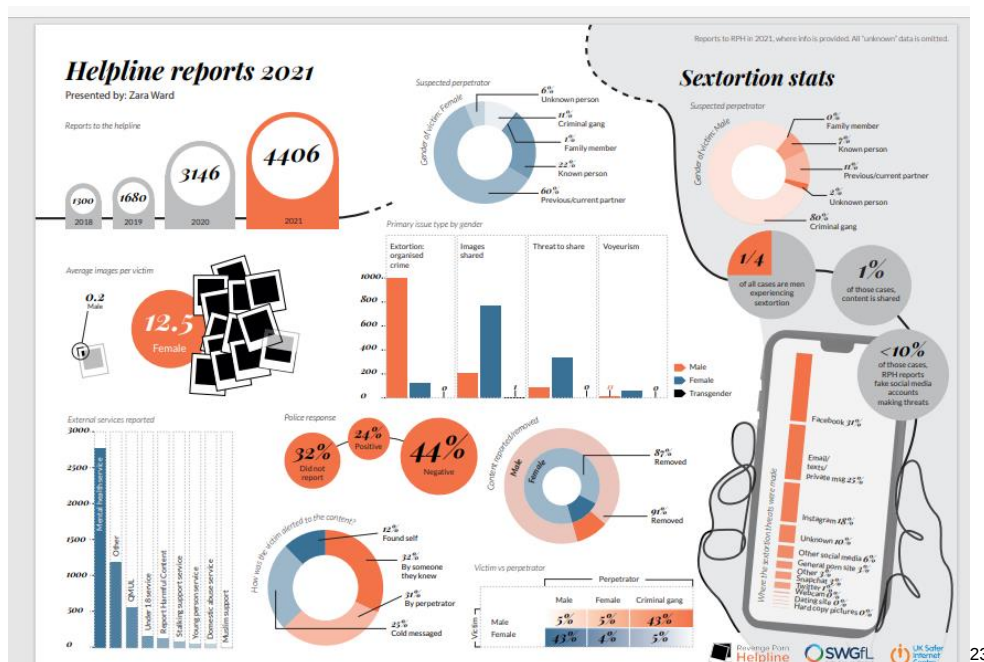
ameaças de divulgação de imagens que nem sempre são verdadeiras, em busca de benefícios para si com finalidades diversas.

“O tipo penal mais assemelhado, pelas características apontadas é o do artigo 216- A do Código Penal, no qual o duplo componente - intenção delinquente e sexo – apresenta- se de forma óbvia”. (SYDOW, 2022, p. 600)

As vítimas pelo constrangimento que passam, acabam ficando com medo e cedem as exigências feitas pelos infratores, o que se torna humilhante e com sequelas irreparáveis.

Uma investigação da BBC descobriu que as fotos íntimas das mulheres estão sendo compartilhadas para assediar, envergonhá-las e chantageá-las em grande escala, no aplicativo de mídia social Telegram.²²

Figura 6: Helpline Reports 2021



Fonte: Revenge Porn Helpline (2021)

Uma esperança para resoluções de casos frustrantes acometidos pelo descaso de divulgações de imagens íntimas, passam a ter uma cobertura preventiva de forma eficaz como pede a situação atual, com objetivo de ter diminuição ou até mesmo

²² Telegram: Onde nus femininos são compartilhados sem consentimento - BBC News

²³ Pesquisa e relatórios de ajuda | Linha de ajuda por pornografia de vingança (revengepornhelpline.org.uk)

extinção de tais delitos criminosos que afetam a violação da honra e imagem virtual e na realidade física.

4.3 STOPNCII.ORG

Como StopNCII.org funciona?

- a) Selecione a imagem íntima(s)/vídeo(s) que deseja hashed do seu dispositivo.
- b) Para cada conteúdo, StopNCII.org gerará uma impressão digital, chamada de 'hash' em seu dispositivo. Apenas o hash é enviado para StopNCII.org, a imagem ou vídeo associado permanece em seu dispositivo e não é carregado.
- c) Se o seu caso for criado com sucesso, você receberá um número de caso para verificar o status do seu caso – lembre-se de fazer uma anotação do número do seu caso junto com o PIN, para acessar seu caso depois que ele for enviado. Isso não é recuperável.
- d) As empresas participantes procurarão correspondências para o hash e removerão quaisquer correspondências dentro de seus sistemas se violarem sua política de abuso de imagem íntima.
- e) Você pode usar seu número de caso a qualquer momento para verificar o andamento do seu caso, ou se deseja retirar sua participação.²⁴

Um dos zelos que merece ser clamado é um investimento mais assíduo nas políticas públicas voltada a atividades educativas para a sociedade com temas voltados ao meio virtual, de forma explicativa de utilização das ferramentas tecnológicas, como também de como se prevenir de forma eficaz contra os crimes virtuais no contexto geral. Direito esse que está expresso na Lei nº 13.853, de 8 de julho de 2019

Art. 55-j. compete à ANPD:

VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;²⁵

²⁴ Pare o abuso de imagem íntima não consensual - StopNCII.org

²⁵ L13853 (planalto.gov.br)

Apesar de ser notório o desinteresse das empresas de investimentos em políticas públicas, já que tais medidas não traz renda lucrativa no mercado digital, que ao analisar todo o conjunto histórico da tecnologia a fonte basilar de todas as criações de ferramentas tecnológicas está voltada diretamente para a lucratividade.

5 CONSIDERAÇÕES FINAIS

O desenvolvimento do presente trabalho possibilitou uma análise da evolução tecnológica que vem mexendo com o mundo no contexto geral, ficando claro que veio para ficar, tendo continuidade cada vez mais complexa na sociedade. A inclusão digital não é mais uma escolha e sim uma necessidade presente nas nossas vidas tornando-se uma fonte essencial e dependente outorgando a impossibilidade de renunciar à tecnologia.

Ao realizar pesquisas bibliográficas voltada ao Direito Digital com foco nos crimes digitais foi possível constatar o tamanho da proporção do alcance do mundo virtual e como tem um poder de modificar as condutas humanas de forma assertiva como também o inverso causando danos pertinentes perante a sociedade. Dessa forma reforça o questionamento do ordenamento jurídico brasileiro que por diversas vezes se torna inoperante diante da fragilidade dos vulneráveis expostos a criminalidade virtual promovendo a impunidade aos infratores cumpridores de condutas infames.

O Objetivo central da presente pesquisa foi aguçar de forma intensificada a importância do conhecimento e aperfeiçoamento das leis que regem os direitos e deveres dos usuários e provedores que fazem parte dessa era digital, frisando a dificuldade da aplicação da legislação brasileira nos crimes virtuais e a defasagem das políticas públicas voltada ao ambiente virtual oferecendo juntamente capacitações para os profissionais policiais e os legisladores se manter atualizados e aptos para elaboração das leis de cobertura tecnológica.

A dificuldade na elaboração desse trabalho se teve relacionado a pouca produção de conteúdo de qualidade com o tema apresentado, por ser ainda uma temática contemporânea que vem inovando constantemente, isso faz com que os próprios especialistas da área passem a ter dificuldades de acompanhamento em tempo real dos fatos ocorridos no mundo digital. Outro fator que trouxe limitações de dados foi a escassez de publicidade em respeito ao segredo de justiça vedando sua publicação.

Portanto, conclui-se que apesar de terem sido realizadas atualmente modificações voltadas a respeito dos crimes virtuais, mesmo assim ainda não são suficientes para se ter uma cobertura total capaz de desencorajar os criminosos na

realização de violações dos direitos dados a sociedade que são retirados pela audácia desses delinquentes.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSIS E MENDES. **Direito Digital, Empresarial e Proteção de Dados**. Disponível em: < <https://assisemendes.com.br/historico-protecao-de-dados/> >. Acesso em: 20 de maio de 2022.

BITTAR, E. C. B. **Introdução ao estudo do direito**. 3. ed. São Paulo: Saraiva, 2022. E-book.

BRASIL. Planalto. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016]. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm >. Acesso em: 20 de maio de 2022.

_____. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal: Centro Gráfico, 1988. 292 p.

CADICRIM, **Crime de perseguição (stalking) artigo 147-a do código penal lei nº 14.132/2021**. Disponível em : STALKING-LEI14.132-2021.pdf (tjsp.jus.br) Acesso em 04 de junho de 2022.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**. 1ª ed. Rio de Janeiro: Brasport, 2014.

DATAREPORTAL. **DIGITAL 2022**. Disponível em: Digital 2022: Brasil — DataReportal – Global Digital Insights . Acesso: 04 de junho de 2022

ESTEFAM, A. **Direito penal**. 10. ed. São Paulo: Saraiva, 2021. E-book.

_____. **Direito penal**. 11. ed. São Paulo: Saraiva, 2022. E-book.

FIORILLO, C, A, P; CONTE, C, P. **Crimes no meio ambiente digital: e a sociedade da informação** 2.ed. São Paulo: Saraiva, 2016.

HELPLINE, revenge porn. **StopNCII.org** . Disponível em: < StopNCII.org lançou | Linha de ajuda por pornografia de vingança (revengepornhelpline.org.uk) > Acesso em: 27 de maio de 2022.

INFOMONEY, Brasil é 5º maior alvo de ciber Crimes no mundo. Disponível em: Brasil é 5º maior alvo de ciber Crimes no mundo - InfoMoney. Acesso em: 04 de junho de 2022.

JESUS, Damásio Evangelista de. **Manual de Crimes Informáticos**. 1ª ed. São Paulo: Saraiva, 2016.

JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos- Ameaças e procedimentos de investigação**. Rio de Janeiro: Braspot, 2012;

KUNRATH, Josefa Cristina. **A expansão da Criminalidade no ciberespaço**. Disponível em: < <http://www.progesp.ufba.br/sites/progesp.ufba.br/files/dissertacao->

final-josefa-cristina-tomaz-martins-kunrath-2014.pdf >. Acesso em: 16 de maio de 2022.

LOPES JUNIOR, Aury. **Direito Processual Penal**. 14 ed. São Paulo: Saraiva, 2017.
MACIEL, K. R. F. L. A. **Curso de direito da criança e do adolescente**. 14. ed. São Paulo: Saraiva, 2022. E-book.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. Editora Saraiva, 2014.

MORAES, Paulo. **Mente Anti-hacker - Proteja-se!** Rio de Janeiro: Brasport, 2011.

NADER, Paulo. **Introdução ao Estudo do Direito**. 36ª Edição. Rio de Janeiro: Editora Forense, 2014.

NUCCI, Guilherme de Souza, **Manual de direito penal**. 10. ed. rev., atual. e ampl. – Rio de Janeiro: Forense, 2014.

_____. **Manual de direito penal**. 16. ed. – Rio de Janeiro: Forensse, 2020.

PACELLI, Eugênio. **Curso de Processo Penal**. – 21. ed. rev., atual. e ampl. – São Paulo: Atlas, 2017;

PATROCINIO. **Divulgação não autorizada de imagens íntimas: experiências de mulheres e de cuidados em saúde**. Belo Horizonte, 2022.

PINHEIRO, P. P. **Direito Digital**. 6. ed. São Paulo: Saraiva, 2015. E-book.

_____. **Direito Digital**. 7. ed. São Paulo: Saraiva, 2021.

_____. Planalto **LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012**. Disponível em: < L12737 (planalto.gov.br) > Acesso em: 21 de maio de 2022.

_____. Planalto. **LEI Nº 14.155, DE 27 DE MAIO DE 2021**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm > Acesso em: 21 de maio de 2022.

_____. Planalto. **LEI Nº 8.069, DE 13 DE JULHO DE 1990**. Disponível em: < L8069 (planalto.gov.br) > Acesso em: 27 de maio de 2022.

_____. Planalto. **LEI Nº 13.853, DE 8 DE JULHO DE 2019**. Disponível em: < L13853 (planalto.gov.br) > Acesso em: 21 de maio de 2022.

_____. Planalto. **DECRETO Nº 7.962, DE 15 DE MARÇO DE 2013**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm > Acesso: 20 de maio de 2022.

_____. Planalto. Decreto-lei nº 3.689, de 3 de outubro de 1941. **Código de Processo Penal** Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm > Acesso em: 14/05/2022.

_____. Planalto. **LEI Nº 13.964, DE 24 DE DEZEMBRO DE 2019**. Disponível em: <L13964 (planalto.gov.br) > Acesso em: 27 de maio de 2022.

_____. Planalto. **LEI Nº 14.132, DE 31 DE MARÇO DE 2021** . Disponível em: < L14132 (planalto.gov.br) > Acesso em: 27 de maio de 2022.

REALE, Miguel, **Filosofia do direito** / 3ª tiragem - 19. ed. - São Paulo Saraiva, 2002.
_____. **Senado** Federal. Emenda Constitucional n 115, 10 de fevereiro de 2022.
Disponível em :<<https://legis.senado.leg.br/norma/35485358/publicacao/35485850> >
Acesso em: 02/05/2022.

SAFERNET. **Sextorsão: eu quero que as pessoas conheçam a minha história**. Disponível em:<https://new.safernet.org.br/content/sextorsao-eu-quero-que-pessoas-conhecam-minha-historia> Acesso em: 06 de junho de 2022

SANTAELLA, L. **Navegar no ciberespaço: o perfil cognitivo do leitor imersivo**. São Paulo: Paulus, 2004.

SANTOS, Altamiro José dos. **Direitos Do Consumidor**. Revista do IAP. Curitiba, Instituto dos Advogados do Paraná, 1987. n. 10.

SERVICE, BB word. Telegram: **Onde os nus das mulheres são compartilhados sem consentimento**. Disponível em: <_Telegram: Onde nus femininos são compartilhados sem consentimento - BBC News > Acesso: 27 de maio de 2022.

SKINNER, B. F. (1976). **About Behaviorism**. New York: Vintage Books. (Trabalho original publicado em 1974)

STOPNCII.ORG. **Pare o abuso de imagem íntima não consensual** . Disponível em: < Pare o abuso de imagem íntima não consensual - StopNCII.org > Acesso em: 28 de maio de 2022.

SYDOW, Spencer Toth, **Curso de Direito Penal Informático**.3. ed. Salvador: Editora JusPodivm, 2022.

SYDOW, Spencer Toth; CASTRO, Ana Lara Camargo. **Exposição Pornográfica não Consentida na Virtualidade: pornografia de vingança, fake nude, sextorsão e outras realidades**. São Paulo: Editora JusPodivm, 2022.

TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de Direito Processual Penal**: de acordo com a Lei nº 12.760/2012 que aumentou o rigor da “Lei Seca”. 8º Edição. Bahia: JusPodvm, 2013.

TEFFÉ, Chiara Spadaccini de. **Exposição não consentida de imagens íntimas: como o direito pode proteger as mulheres?** In: ROSENVALD, Nelson; DRESCH, Rafael de Freitas Valle; WESENDONCK, Tula (coord.). Responsabilidade civil: novos riscos. Indaiatuba: Editora Foco, 2019. p. 94-95.

TEIXEIRA, T. **Comércio eletrônico - Conforme o Marco Civil da Internet e a regulamentação do e-commerce no Brasil**. São Paulo: SARAIVA, 2015. E-book.

_____. **Direito Digital e Processo Eletrônico**. 5. ed. São Paulo: Saraiva, 2020. E-book.

WACHOWICZ, Marcos **Proteção de dados pessoais em perspectiva: LGPD e P967 RGPD na ótica do direito comparado** / Curitiba: Gedai, UFPR 2020.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos**. São Paulo: Brasport, 2012.

WHITAKER, F. Rede – **Uma Estrutura Alternativa de Organização**. Rio de Janeiro: Revista Mutações Sociais. CEDAC, ano 2, n. 3, março/abril/maio de 1993.