



Universidade de Brasília – UnB
Faculdade de Direito – FD
Programa de Graduação em Direito

**A TUTELA CONSTITUCIONAL-CIVIL DA IDENTIDADE DIGITAL:
LETRAMENTO DIGITAL DO TITULAR DA CIBERIDENTIDADE COMO UM
MECANISMO ANTIFRAUDE**

JOELANE RODRIGUES CARVALHO

Brasília

2023

JOELANE RODRIGUES CARVALHO

**A TUTELA CONSTITUCIONAL-CIVIL DA IDENTIDADE DIGITAL:
LETRAMENTO DIGITAL DO TITULAR DA CIBERIDENTIDADE COMO UM
MECANISMO ANTIFRAUDE**

Monografia apresentada como requisito parcial para a
obtenção do grau de Bacharela em Direito pelo
Programa de Graduação da Faculdade de Direito da
Universidade de Brasília (FD-UnB).

Orientadora: Ma. Eduarda Moraes Chacon Rosas

Brasília

2023

Autorizo a reprodução e divulgação total ou parcial deste trabalho, por qualquer meio convencional ou eletrônico, para fins de estudos e pesquisa, desde que citada a fonte.

RC331 Rodrigues Carvalho, Joeline
 / Joeline Rodrigues Carvalho; orientador Eduarda Moraes
 Chacon Rosas . -- Brasília, 2023.
 106 p.

 Monografia (Graduação - A tutela constitucional-civil da
 identidade digital: letramento digital do titular da
 ciberidentidade como um mecanismo antifraude) --
 Universidade de Brasília, 2023.

 1. A ciberidentidade e os riscos da era digital. 2. A
 usurpação de identidade como mecanismo viabilizador da
 fraude. 3. A tutela constitucional-civil da ciberidentidade
 e a responsabilidade do próprio titular. 4. A dimensão
 objetiva da conduta da vítima de fraudes. I. Moraes Chacon
 Rosas , Eduarda , orient. II. Título.

Citar como: CARVALHO, Joeline Rodrigues. *A tutela Constitucional-Civil da Identidade Digital: Letramento digital do titular da ciberidentidade como um mecanismo antifraude*, 2023. 105 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade de Brasília, Brasília, 2023

JOELANE RODRIGUES CARVALHO

A TUTELA CONSTITUCIONAL-CIVIL DA IDENTIDADE DIGITAL
LETRAMENTO DIGITAL DO TITULAR DA CIBERIDENTIDADE COMO UM
MECANISMO ANTIFRAUDE

Monografia apresentada como requisito parcial para a obtenção do grau de Bacharela em Direito pelo Programa de Graduação da Faculdade de Direito da Universidade de Brasília (FD-UnB).

Orientadora: Ma. Eduarda Moraes Chacon Rosas

Aprovada em 06 de dezembro de 2023

BANCA EXAMINADORA

Mestra Eduarda Moraes Chacon Rosas

Faculdade de Direito da Universidade de Brasília (FD-UnB)

Orientadora - Presidente

Professor Doutor Alexandre Kehrig Veronese Aguiar

Faculdade de Direito da Universidade de Brasília (FD-UnB)

Examinador

Professor Doutor Victor Marcel Pinheiro

Universidade de São Paulo (USP)

Examinador

Brasília

2023

*À minha mãe, Antônia, que me educou no caminho do direito;
Ao meu pai, Carvalho, que me ensinou a pensar direito desde pequenina;
À minha irmã, Cind, com quem eu caminho direito.*

AGRADECIMENTOS

Nos inúmeros trabalhos acadêmicos que li na minha graduação, uma ação virou regra: o início da leitura pelos agradecimentos. Chorei em muitos, ri em tantos outros... Enquanto isso, na minha mente, tentava antecipar a árdua tarefa que seria resumir em poucos parágrafos a eterna gratidão que tenho por todos que me acompanharam até aqui.

E, como não construímos nada sozinhos, escolhi os melhores para estarem ao meu lado. Como disse uma série notável, a seleção das pessoas ao nosso redor é o mais próximo que chegamos de delinear nosso destino.

Assim, agradeço imensamente aqueles que me apoiaram de forma significativa para a conclusão desta monografia – um marco em minha jornada acadêmica no curso de Direito da Universidade de Brasília (UnB). Gostaria, também, de expressar minha gratidão especial a algumas pessoas que foram essenciais ao longo deste percurso, pois sem elas certamente não teria sido possível realizar este feito.

Primeiramente, gostaria de agradecer a minha mãe, **Antônia**, por sempre ter priorizado a minha educação, nunca medindo esforços para que eu tivesse acesso a melhor instrução possível. Você é o suporte que permite que todas as minhas conquistas aconteçam. Essa vitória é nossa!

À meu pai, **Carvalho**, pelo apoio incondicional nos dias que precisei estender os estudos por algumas horas a mais da madrugada.

À minha irmã, **Cind**, meu primeiro exemplo acadêmico. Quem me acompanhou nas inúmeras provas e entrevistas de programas de bolsas de estudos que fiz ao longo da vida. Obrigada pelas palavras de confiança e por sempre me ensinar que a vida é mais que os estudos, mesmo quando, às vezes, me sentia desmotivada.

Deixo, igualmente, um agradecimento aos meus sobrinhos: **Maria Laura, João Marcelo e Elena**, que carregam não apenas um sobrenome igual ao meu, mas a expectativa e esperança de uma geração que tenha na educação um de seus principais pilares. Depois de entender a responsabilidade e a potencialidade de “ser tia/madrinha”, entendi que precisaria sempre dar o meu melhor, por e para vocês.

Aos primos e tios, agradecimento que faço no nome das minhas tias **Maria Eugênia, Uilima e Lucena**. Agradeço a compreensão pelos momentos em que foi necessária a minha ausência, a fim de que pudesse me dedicar aos estudos e por todo o apoio e momentos de alegria.

À minha avó, **Antônia Saraiva**, por me fazer acreditar, a cada dia, na importância da família. Ela, que me trouxe pela primeira vez até Brasília, cidade que me acolheu nestes últimos

6(seis) anos. Gostaria de dizer que compreendo que a família seja grande, e as demandas sejam muitas. Justamente por isso, agradeço por toda a torcida convertida em oração e promessa. Elas deram certo! Estamos aqui!

Às minhas melhores amigas de ensino médio: **Talita Carneiro e Luanna Kellen**. Obrigada por todas as risadas e pela companhia incrível nestes últimos 10 anos. À meus amigos da Faculdade de Direito: **Gabi, Carlos, Duda, Sarah e Will**. Obrigada por me incentivarem a ser uma pessoa melhor e comemorarem comigo cada vitória conquistada na graduação. Fico honrada em saber que acompanho excelentes profissionais.

Estendo estes agradecimentos aos amigos que encontrei na vida profissional: **Fausto Neiva, Jean Borges e Luiz Vinicius**. Vocês foram minhas primeiras referências profissionais. Obrigada por escutarem minhas longas histórias, piadas e, sobretudo, por me apoiarem sempre. A trajetória de vocês, com certeza, será brilhante.

Aos amigos que a diretoria da **Advocatta EJ** me deu e o **Observatório da LGPD** manteve. Obrigada pelas sugestões, conversas, artigos e pela parceria acadêmica. Espero que continuemos nossa jornada pela Privacidade e Proteção de Dados juntos.

À minha amiga, **Letícia Rejane**, pela companhia de estudos na Biblioteca Central da UnB e por ser minha motivação diária na Faculdade de Direito. Sua contribuição foi essencial para a finalização deste trabalho e para o término bem-sucedido da minha graduação.

À todos os **funcionários, servidores e professores** excepcionais com quem tive o privilégio de compartilhar os últimos cinco anos de estudo. Vocês são uma fonte contínua de inspiração em minha jornada.

Aos Srs. **Victor Marcel e Alexandre Veronese** por aceitarem o convite para integrar a banca de avaliação da minha monografia, mesmo diante de suas agendas tão ocupadas. A contribuição do conhecimento de vocês será de extrema importância para o meu crescimento acadêmico.

À meus colegas de profissão, sobretudo minha advogada e orientadora, **Eduarda Moraes Chacon Rosas**, que acreditou em mim profissionalmente e me concedeu um novo olhar acerca da advocacia. Sua disponibilidade, sua paciência, sua empatia, seu carinho e seu comprometimento foram essenciais para aprimorar meu trabalho e me guiar na busca por conhecimento.

Aos demais amigos do **BFBM Advogados**: estagiários, advogados, trainees e funcionários. Obrigada por me acolherem e concederem a liberdade de encontrar no BFBM muito mais que um ambiente de trabalho. Vocês foram o meu alicerce nestes últimos dois anos.

À minha melhor amiga de profissão, **Amanda Melo**, você me inspira a ser uma pessoa melhor todos os dias. Obrigada por cada conselho dado, por cada vídeo divertido enviado, pela companhia diária no cafezinho da tarde e nos treinos de musculação. Você foi o maior presente que eu poderia ter ganhado nos últimos tempos.

Por fim, reitero meus agradecimentos à **Universidade de Brasília** e a todos que lutam por um ensino público de qualidade. Em nenhum momento tive dúvidas de que a escolha de fazer parte desta instituição foi a mais acertada da minha vida acadêmica.

Que este momento de gratidão seja apenas o começo de uma trajetória animada e repleta de conquistas para todos nós. Muito obrigada por tudo!

Com amor, Joe.

RESUMO

Com o advento da economia de dados e das sociedades de informações, os indivíduos passaram a se questionar sobre a proteção – e vulnerabilidade – de suas identidades no ciberespaço. Isso porque, a era digital tem intensificado uma crise que vinha sendo anunciada desde os primórdios da pós-modernidade: a fragilidade da proteção dessa faceta da identidade, que para os efeitos desse trabalho denominar-se-á digital. Este paradigma tem franqueado a demanda para que o direito e os princípios e regras jurídicos que o edificam estejam constantemente se adaptando – não apenas pelas possibilidades tecnológicas, mas também pela transformação que causa na mentalidade e no comportamento humano. É diante deste panorama que esta monografia se propõe a analisar a proteção da identidade digital focando na usurpação de identidade enquanto ilícito civil que compreende a obtenção e a utilização indevida de dados por terceiros para o cometimento de fraudes. A metodologia contou com métodos de pesquisa exploratória, documental, doutrinária e jurisprudencial; equacionando bases de dados relativas às áreas do Direito – especificamente Constitucional, Civil e Consumerista. A análise se desdobrará em tópicos, abordando (i) a matriz do direito à identidade; (ii) a usurpação de identidade como facilitadora de fraudes online e (iii) a tutela da ciberidentidade no direito civil e do consumidor. Se concluirá, em termos de responsabilização civil, que a apropriação indevida da identidade pessoal digital pode ser sancionada a partir do atual sistema legal. De outro lado, tendo em vista que parte dos delitos é facilitada pelo próprio ofendido por falta de informação e cautela, é necessário repensar – no macrocenário do fomento à livre iniciativa e ao desenvolvimento econômico – em limites para a delegação da (ir)responsabilidade deles a fornecedores de serviços; e em políticas públicas de prevenção a fraudes via letramento digital dos cidadãos.

Palavras-chave: ciberidentidade; identidade digital; fraude; responsabilidade civil; dados pessoais

ABSTRACT

With the advent of the data economy and information societies, individuals have begun to question the protection – and vulnerability – of their identities in cyberspace. This is because the digital era has intensified a crisis that has been announced since the early days of post-modernity: the fragility of protecting this facet of identity, referred to as digital for the purposes of this work. This paradigm has opened the door for the demand that the law and the principles and legal rules that underpin it constantly adapt – not only due to technological possibilities but also because of the transformation it causes in human mentality and behavior. It is in this context that this thesis aims to analyze the protection of digital identity, focusing on identity theft as a civil offense that involves the unauthorized acquisition and use of data by third parties for the commission of fraud. The methodology employed exploratory, documentary, doctrinal, and jurisprudential research methods; balancing databases related to legal areas – specifically Constitutional, Civil, and Consumer Law. The analysis will unfold in topics, addressing (i) the framework of the right to identity; (ii) identity theft as a facilitator of online fraud; and (iii) the protection of cyber-identity in civil and consumer law. In terms of civil liability, it will be concluded that the improper appropriation of digital personal identity can be sanctioned under the current legal system. On the other hand, considering that part of the offenses is facilitated by the victims themselves due to lack of information and caution, it is necessary to rethink – in the larger context of promoting free enterprise and economic development – limits for delegating their (ir)responsibility to service providers; and public policies to prevent fraud through digital literacy education for citizens.

Keywords: cyber identity; digital identity; fraud; liability; personal data

LISTA DE FIGURAS

Figura 1: Processo de julgamento público do risco	29
Figura 2: Quanto custa o cibercrime?	35
Figura 3: Pesquisa sobre “roubo” de identidade na internet	36
Figura 4: Pesquisa por estratificação - Identidade roubada internet	37
Figura 5: Cibercrimes no contexto de Obtenção x Utilização Indevida de Dados Pessoais	43
Figura 6: O ciclo da engenharia social	44

LISTA DE TABELAS

Tabela 1: Atributos das tecnologias digitais e suas implicações no campo da responsabilidade Civil	59
Tabela 2: Teorias de análise do nexu causal na Responsabilização Civil	61
Tabela 3: Excludentes de Causalidade - Caso Fortuito, Força Maior, Culpa exclusiva da Vítima e Fato de Terceiro	62
Tabela 4: Principais tipos de danos relacionados à usurpação de identidade	68
Tabela 5: Parâmetros a serem considerados na análise da responsabilidade do ofendido.	74
Tabela 6: Hipóteses de criação do Autorrisco pelo ofendido	81

LISTA DE ABREVIATURA E SIGLAS

CDC	Código de Defesa do Consumidor
CRFB	Constituição da República Federativa do Brasil
CPC	Código de Processo Civil
LGPD	Lei Geral de Proteção de Dados Pessoais
MCI	Marco Civil da Internet
PIB	Produto Interno Bruto
RE	Recurso Extraordinário
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
TJSP	Tribunal de Justiça do Estado de São Paulo

SUMÁRIO

1. INTRODUÇÃO	14
2. A CIBERIDENTIDADE E OS RISCOS DA ERA DIGITAL.	20
2.1. Onde tudo Começa: A Tutela da Ciberidentidade como corolário do princípio da Dignidade Humana e do Direito Fundamental à proteção de Dados pessoais	20
2.2. A Compreensão da Era Digital no contexto da Sociedade de Riscos	25
2.2.1. <i>Fraudes na Sociedade de Dados e da Informação</i>	34
2.3. A usurpação de identidade como um processo de duas etapas	38
3. USURPAÇÃO DA IDENTIDADE COMO MECANISMO VIABILIZADOR DA FRAUDE	42
3.1. O Phishing como mecanismos de uso indevido da identidade alheia	43
3.2. O titular como responsável pela apropriação de sua identidade por terceiros: Smishing e Vishing	45
3.3. A relação entre Falsificação de documentos e a usurpação da identidade digital	46
3.4. Identidades digitais falsas e o Catfishing	47
3.5. A identidade digital como elemento essencial da personalidade do indivíduo na sociedade de dados e a sua fragilidade: o que é preciso pensar em termos de construção de uma tutela eficaz e que papel o titular exerce neste cenário?	48
4. A TUTELA CONSTITUCIONAL-CIVIL DA CIBERIDENTIDADE E A RESPONSABILIDADE DO PRÓPRIO TITULAR	49
4.1. Diálogo entre a proteção de identidade digital e a responsabilidade civil: panorama histórico-teórico	49
4.2. A proteção da ciberidentidade no contexto da sociedade de dados: O direito precisa assimilar a realidade algorítmica e suas consequências práticas	54
4.3. A tutela da vítima de danos: uma análise a partir dos pressupostos da Responsabilidade Civil	57
4.3.1. <i>Ato ilícito</i>	57
4.3.2. <i>O nexa causal: Prova de prejuízos e dificuldades na reparação</i>	58

<i>4.3.3. O dano plurifacetado</i>	64
<i>4.3.5. O dano moral e o Titular de Dados Pessoais</i>	68
<i>4.3.6. A culpa e o risco no regime de responsabilidade</i>	71
4.4. A dimensão objetiva da conduta da vítima de Fraudes	72
<i>4.4.1. Consentimento do Lesado</i>	76
<i>4.4.2. Autocolocação da Vítima em Risco</i>	79
4.6. A má gestão de segurança da identidade digital pelo titular, ou dos mecanismos que dispunha para protegê-la, como excludente (integral ou parcial) de responsabilidade civil do agente de tratamento, provedor ou fornecedor em cujo sistema o criminoso se passou por ele.	89
5. CONCLUSÃO	92
REFERÊNCIAS	97

1. INTRODUÇÃO

Para a análise eficiente da tutela da ciberidentidade, no atual cenário regulatório, faz-se necessário antes de nada fazer um recorte teórico-metodológico. Este trabalho se limitará a questionar e ponderar sobre a questão no limite das legislações postas, em especial as regras de proteção de dados e governança da privacidade.

Considerado este ângulo, se observará como a defesa da privacidade e da proteção de dados são historicamente tratadas no Brasil e em outras nações. Isso porque, a hipótese aqui proposta é de que a proteção da identidade digital hoje, sobretudo para os fins aos quais este trabalho se propõe, deve se preocupar e se ocupar com a usurpação de identidade. A seu turno, esta perpassa por duas fases essenciais: (i) a obtenção dos dados (lícita ou ilícitamente; correspondente ao *identity theft*) (ii) que tenha como propósito o uso indevido (não autorizado) por terceiros para práticas ilícitas (*identity fraud*).

Com esse objetivo, parte-se de um marco direcionado à compreensão do constructo da temática da privacidade no mundo, expondo também como a internet – e o lampejo da necessidade de se criar um ordenamento que inclua a proteção de dados pessoais nesse meio – franqueou a demanda por adaptações nos sistemas de responsabilidade e de reparação às vítimas de ilícitos praticados no ambiente cibernético (especialmente no Brasil).

Tendo em vista a extensão da temática, sobretudo na área jurídica, centralizar-se-á o estudo em uma abordagem constitucional-civil do ilícito de usurpação de identidade e suas consequências. Sobretudo porque, compreende-se que a garantia de que o indivíduo, em tese, possa ser e estar seguro no ambiente virtual é uma forma de salvaguardar e estender a aplicação do princípio da dignidade da pessoa humana e do livre exercício do direito da personalidade no ambiente digital.

E se por um lado a identidade pessoal caminhou paralelamente ao princípio constitucional da dignidade da pessoa humana em diversos julgados paradigmas no Judiciário brasileiro - como aquele que reconheceu o direito ao nome¹ e o que analisou a possibilidade de

¹ A relevância constitucional do direito à identidade e ao nome foi proclamada pelo Supremo Tribunal Federal no julgamento do RE 248.869. Naquele julgado, ao se reconhecer a constitucionalidade da legitimidade ativa do Ministério Público para ajuizamento, após provocação, de demanda de investigação de paternidade, foi frisada a íntima conexão entre o direito ao conhecimento da própria origem biológica e a dignidade da pessoa humana, conforme ementa da lavra do rel. min. Maurício Corrêa (*in memoriam*), verbis: “3. O direito ao nome insere-se no conceito de dignidade da pessoa humana e traduz a sua identidade, a origem de sua ancestralidade, o reconhecimento da família, razão pela qual o estado de filiação é direito indisponível, em função do bem comum maior a proteger, derivado da própria força impositiva dos preceitos de ordem pública que regulam a matéria”

repropositura de ação de paternidade pela busca da identidade genética² -, por outro lado, sabe-se que com a repersonalização do direito civil, deu-se maior destaque aos direitos da personalidade no panorama do direito privado.

É diante desse contexto que o direito à identidade pessoal e digital exsurge como uma novidade no âmbito dos direitos da personalidade. Isso decorre da demanda por uma proteção mais robusta da "verdade pessoal" que inclui informações de identificação, mas também evoluiu para abranger aspectos mais subjetivos de autorreconhecimento de posições identitárias. Com efeito, a pergunta que logo surge é: e por que o direito à preservação da ciberidentidade é necessário?

De antemão, pode-se argumentar que sua finalidade é garantir a dignidade humana. Num segundo momento, quando a definição de identidade se vinculará ao conjunto de características próprias, pode justificar uma proteção à privacidade pessoal. Tais respostas, não obstante, mostram-se vagas e genéricas, uma vez que os direitos fundamentais e muitos outros direitos também tendem a compartilhar dessa mesma finalidade (preservação da dignidade da pessoa humana e/ou da privacidade pessoal).

Assim, compreende-se que a razão fundamental da tutela de direito à identidade pessoal digital é permitir o livre exercício da individualidade por meio do digno desenvolvimento da

Ministério Público Estadual. **RE 248.869-1/SP**. 7 ago. 2003. Disponível em: <<https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=257829>>. Acesso em: 20 nov. 2023

No mesmo sentido: “(...) 106. O nome como um atributo da personalidade, constitui uma expressão da individualidade e visa afirmar a identidade de uma pessoa perante a sociedade e as ações contra o Estado. Com ele, procura-se conseguir que cada pessoa tenha um sinal distintivo e singular frente às demais, com o qual pode ser identificado e reconhecido. É um direito fundamental inerente a todas as pessoas pelo simples fato de sua existência. Além disso, este Tribunal indicou que o direito ao nome (reconhecido no art. 18 da Convenção e também em vários instrumentos internacionais) constitui um elemento básico e indispensável da identidade de cada pessoa, sem o qual ela não pode ser reconhecida pela sociedade nem registrada perante o Estado. (...) 115. (...) Isso significa que os Estados devem respeitar e garantir a toda pessoa a possibilidade de registrar ou de mudar, retificar ou adequar seu nome e os demais componentes essenciais de sua identidade, como a imagem, ou a referência ao sexo ou gênero, sem interferência das autoridades públicas ou de terceiros”. In: **Corte IDH. OC 24/2017**, Parecer consultivo sobre identidade de gênero, igualdade e não discriminação entre casais do mesmo sexo, de 24-11-2017, solicitado pela República de Costa Rica. [Tradução livre]. Disponível em: https://www.corteidh.or.cr/docs/opiniones/seriea_24_por.pdf. Acesso em: 20 nov. 2023

² No julgamento do RE n.363.889, sob a relatoria do Min. Dias Toffoli, que tinha como objeto a análise do reconhecimento da impossibilidade do prosseguimento de ação de investigação de paternidade, com fundamento em coisa julgada, dado o ajuizamento de anterior demanda, com o mesmo objeto, cuja sentença de improcedência já havia transitado em julgado; o MM. Magistrado destacou que a construção da identidade pessoal sofreu forte influxo pelo desenvolvimento das pesquisas em torno do genoma humano passando “a ser concebida como o complexo de elementos que individualizam cada ser humano, distinguindo-o dos demais na coletividade, conferindo-lhe autonomia para que possa se desenvolver e se firmar como pessoa em sua dignidade, sendo, portanto e nessa medida, expressão objetiva do princípio da dignidade da pessoa humana”.

Goiá Schmaltz, Diego.; MPDFT. **Recurso Extraordinário 363.889/DF**. 2 jun. 2011. Disponível em: <<https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=1638003>>. Acesso em: 20 nov. 2023.

personalidade, quer seja na esfera física quer seja no âmbito virtual. De forma mais concisa, esses direitos têm como propósito concretizar a identidade pessoal em um projeto seguro e individual de existência.

O direito à identidade pessoal representa uma construção jurídica (em certa medida, uma simplificação) destinada a proteger a singularidade de cada indivíduo, enquadrada dentro dos parâmetros dos direitos da personalidade. Sua evolução é recente e teve início no século XX, durante as décadas de 1970 e 1980, notadamente entre os juristas italianos.

Antes disso, predominava a noção de que a identidade se limitava aos elementos de identificação (documentos, características físicas, sinais distintivos, entre outros)³. Essa perspectiva refletia o paradigma jurídico da época, segundo o qual os interesses ligados ao patrimônio prevaleceriam sobre outras formas de interesse.⁴

Em suas novas formulações teóricas, esse direito recebeu algumas propostas que o denominaram como "direito à identidade moral"⁵ ou ainda "direito de ser si mesmo". Apesar das diversas terminologias, as discussões convergiam para um mesmo ponto: a preocupação com a proteção legal das questões que conferiam singularidade e irrepetibilidade a uma pessoa, ou seja, aquelas características que a distinguem e a qualificam como um indivíduo dotado de uma identidade pessoal exclusiva.⁶

Tal concepção de direito, certamente, foi alvo de críticas e dúvidas. A elaboração jurídica do direito à preservação da (ciber)identidade enfrentou vozes discordantes que, de maneira resumida, questionaram sua classificação como um "novo direito" e a relevância de estabelecer um "direito à identidade pessoal digital" no âmbito dos direitos da personalidade.

³ Neste mesmo sentido é o voto do Ministro Dias Toffoli no julgamento do RE nº 363.889, *litéris*: “na visão tradicional do direito civil, que vigorou até o progresso científico alcançado no último quarto do século passado, a posição particular da pessoa natural no seio social era definida predominantemente por seu nome.” GOIÁ SCHMALTZ, Diego.; MPDFT. **Recurso Extraordinário 363.889/DF**, p.27. Disponível em: <<https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=1638003>>. Acesso em: 20 nov. 2023.

⁴ CHOERI, Raul Cleber da Silva. **O direito à identidade na perspectiva civil-constitucional**. Rio de Janeiro: Renovar, 2010. p. 178.

⁵ Segundo GAMBARO, Antonio. *apud* PINO, Giorgio. Il diritto all'identità personale, *cit.*, pp. 9-10 *apud* CAMPOS, Ligia Fabris. **O Direito de ser si mesmo: a tutela da identidade pessoal no ordenamento jurídico brasileiro**. Dissertação (Mestrado em direito) - Pontifícia Universidade Católica: Rio de Janeiro, PUC-RJ, 2006. p. 50.

⁶ BOLESINA, Iuri.; GERVASONI, Tamiris Alessandra. **O direito à identidade pessoal no Brasil e seus fundamentos jurídicos na atualidade**. v. 8, n. 13, 2018. p. 74.

Este argumento se apoiava no fato de que a proteção da identidade poderia ser, e em certo sentido era, realizada por outros direitos da personalidade já existentes⁷. Levando em conta tais considerações, juristas que se inclinavam a reconhecer a identidade pessoal como um direito, começaram a repensá-lo, especialmente em relação ao seu conceito e à sua aplicação⁸.

Ao resumir a jurisprudência italiana e a opinião predominante, Giorgio Pino⁹ argumentou que o direito à identidade pessoal seria um legítimo direito de proteção que asseguraria o interesse de um indivíduo em não ter sua identidade distorcida ou modificada devido à atribuição de fatos, concepções, opiniões, qualidades ou comportamentos falsos, inexistentes ou divergentes daquilo que o titular realmente possui e/ou expressa, independentemente do impacto em outros direitos da personalidade. Ou seja, tal direito serviria para defender e resguardar o interesse do indivíduo em ser reconhecido como realmente é: sua identidade genuína.

Na Alemanha, o reconhecimento do direito à identidade pessoal (*Recht auf Identität*) ocorreu por meio de decisões judiciais e, similarmente à Itália, se propôs a preservar a autêntica identidade. O alcance da proteção seria, no entanto, mais abrangente, visto que também englobaria as identidades culturais e de grupos, além de reconhecer como direitos derivados do direito à identidade pessoal, o direito à representação da própria imagem existencial (*Lebensbild*) e o direito à livre autodeterminação informativa (*Recht auf informationelle Selbstbestimmung*).

No contexto francês, o direito à identidade pessoal abrangeria tanto os aspectos identificativos distintivos (como nome, data de nascimento) quanto os elementos da individualidade (como opiniões e sentimentos), sempre que fossem objetivamente observáveis na vida social ou em relações interpessoais. Não por acaso, mas precisamente devido a essa dualidade protetiva, o direito em questão é ocasionalmente referido na França como "direito à identidade pessoal (*droit à l'identité personnelle*)" e em outras ocasiões como "direito à autenticidade (*droit à l'authenticité*)"¹⁰.

⁷ BOLESINA, Iuri.; GERVASONI, Tamiris Alessandra. **O direito à identidade pessoal no Brasil e seus fundamentos jurídicos na atualidade**. v. 8, n. 13, 2018. p. 56-68.

⁸ SESSAREGO, Carlos Fernandez. **Derecho a la identidad personal**. Buenos Aires: Austrea, 1992. p. 23-24.

⁹ PINO, Giorgio. Il diritto all'identità personale ieri e oggi. Informação, mercado, dati personali. *In: Libera circolazione e protezione dei dati personali*. [s.l.] Giuffrè Editore, 2006. p. 258 *apud* BOLESINA, Iuri.; GERVASONI, Tamiris Alessandra. **O direito à identidade pessoal no Brasil e seus fundamentos jurídicos na atualidade**. v. 8, n. 13, 2018. p. 75.

¹⁰ PINO, Giorgio. Il diritto all'identità personale ieri e oggi. Informação, mercado, dati personali. *In: Libera circolazione e protezione dei dati personali*. [s.l.] Giuffrè Editore, 2006. p. 265-266 *apud* BOLESINA, Iuri.;

Nos Estados Unidos, o direito à identidade pessoal seria considerado como um desdobramento do direito à privacidade, inserindo-se na salvaguarda contra a divulgação de informações falsas ao público (*false light on the public eye*)¹¹ e na prevenção da apropriação indevida do nome (*misappropriation*)¹². Conforme a mesma orientação europeia, esse direito visaria proteger a pessoa que teve alguma informação, opinião ou comportamento seu divulgado de maneira distorcida perante a comunidade, evitando ou reparando potenciais danos (materiais ou morais)¹³.

Relevante, para o presente estudo, aquela que é a identidade "exteriorizada", ou seja, todos os elementos que distinguem as pessoas como indivíduos (nome, data de nascimento, filiação, cadastro de pessoa física, dentre outros). Afinal, é a partir da apropriação indevida dessa identidade que grande parte dos ilícitos cibernéticos ocorrem.

Quando se menciona o termo usurpação de identidade se faz referência à utilização dessa identidade por terceiros para fins ilícitos. Tem-se observado que este é um fenômeno que cresceu muito nos últimos anos e isso se deve, principalmente, ao aprimoramento de técnicas de fraudes desenvolvidas após o uso da internet. A *web* (*e a deepweb*), como fonte crucial de informação, facilitou consideravelmente a divulgação dos dados de identidade/identificação.

A crescente digitalização dos dados torna a vida cotidiana mais conveniente e eficiente, mas igualmente facilita a prática de comportamentos associados à apropriação indevida de identidade. Nota-se, nesse diapasão, uma "releitura" da ideia de sociedade do risco do sociólogo alemão Ulrich Beck¹⁴.

Beck destaca que o mesmo progresso de modernização que impacta positivamente o desenvolvimento tecnológico e científico, acaba por criar ameaças e outras consequências nocivas ao indivíduo, diante das quais a sociedade deve se modernizar e se organizar em resposta. No cenário ora analisado, as ações danosas que tomaram protagonismo com o advento

GERVASONI, Tamiris Alessandra. **O direito à identidade pessoal no Brasil e seus fundamentos jurídicos na atualidade**. v. 8, n. 13, 2018. p.13

¹¹ PINO, Giorgio. Il diritto all'identità personale ieri e oggi. Informazione, mercato, dati personali. *In*: Libera circolazione e protezione dei dati personali. [s.l.] Giuffrè Editore, 2006. p.267 *apud* BOLESINA, Iuri.; GERVASONI, Tamiris Alessandra. **O direito à identidade pessoal no Brasil e seus fundamentos jurídicos na atualidade**. v. 8, n. 13, 2018. p.13.

¹² CHOERI, Raul Cleber da Silva. **O direito à identidade na perspectiva civil-constitucional**. Rio de Janeiro: Renovar, 2010. p. 220.

¹³ CAMPOS, Ligia Fabris. **O Direito de ser si mesmo**: a tutela da identidade pessoal no ordenamento jurídico brasileiro. Dissertação (Mestrado em direito) - Pontifícia Universidade Católica: Rio de Janeiro, PUC-RJ, 2006. p. 82.

¹⁴ BECK, Ulrich. **Sociedade de risco mundial**: em busca da segurança perdida. Edições 70, 448p, 2015.

da internet organizam-se no conceito de *cibercrime* (*ciberilícitos*), lesionando bens jurídicos e violando a privacidade e a proteção de dados pessoais no ambiente virtual.¹⁵

Frente a essa conjuntura, levanta-se a seguinte indagação: a humanidade caminha rumo à proteção da ciberidentidade com a mesma velocidade com que está progredindo a inteligência artificial e as tecnologias de “facilitação” de rotina?

O propósito desta pesquisa é, portanto, investigar as ameaças que acompanham os progressos tecnológicos, com foco particular na questão da usurpação de identidade digital, e compreender se as leis e regulamentos estão eficazmente lidando com as novas formas de ciberdelitos, bem como se são suficientes à proteção das vítimas.

Na metodologia empregada, adota-se a pesquisa exploratória, documental, doutrinária e jurisprudencial; equacionando bases de dados relativas às áreas do Direito – especificamente Constitucional, Civil e Consumerista. A técnica de pesquisa utilizada consiste na documentação indireta por meio da revisão bibliográfica. O ponto de partida deste projeto é, por sua vez, a compreensão do direito à preservação da identidade pessoal digital sob a perspectiva de um direito e garantia fundamental que se concretiza não apenas como expressão da dignidade da pessoa humana, mas também como direito à proteção de dados pessoais subjacente ao princípio do livre desenvolvimento da personalidade.

Na sequência, o caminho de desenvolvimento traçado será: No primeiro tópico analisar-se-á a matriz do direito à identidade como corolário dos direitos fundamentais à igualdade, à privacidade e à dignidade humana. No segundo tópico, a usurpação de identidade enquanto mecanismo viabilizador de fraudes online. No terceiro tópico, o objeto de estudo será a tutela da identidade a partir da perspectiva do direito civil e do código de defesa do consumidor, identificando os maiores obstáculos para a reparação de danos sofridos por estas vítimas. Nele, com a licença da teoria geral do direito penal, será apresentada a vitimodogmática¹⁶ que servirá

¹⁵ CALLEGARI, André Luís; ANDRADE, Roberta Lofrano. **Sociedade do risco e direito penal**. Revista da Defensoria Pública do Estado do Rio Grande do Sul, n. 26, 2020. p. 115–140.

¹⁶ A doutrina apresenta divergências em relação à compreensão do conceito de vitimodogmática, o que pode comprometer a clareza de seu escopo. No entanto, mesmo diante dessa variedade de interpretações, é possível identificar pontos convergentes nessas abordagens. O primeiro destes pontos refere-se à observação empírica da contribuição de algumas vítimas para a afetação de seus próprios interesses jurídicos. O segundo ponto circunscreve-se à valoração desse comportamento dentro do campo da dogmática jurídico-penal, com o objetivo preciso de determinar em que medida essa conduta pode impactar a culpabilidade do agente. In: CORDEIRO, Euller Xavier. Vitimodogmática: Uma análise dogmática do comportamento da Vítima. In: FALEIROS JÚNIOR, Roberto Galvão. (Ed.). **Estudos contemporâneos de vitimologia**. São Paulo: Cultura Acadêmica: Editora UNESP, 2011. p. 25–75.

de instrumento para o cotejo da tutela do Estado face à danosidade e a “contribuição” que a vítima tem no delito deflagrado.

Ao término da análise, se confirmará se a imputação de responsabilidade civil por danos morais (e materiais) resultantes da apropriação indevida da identidade pessoal digital é viável sob o atual arcabouço legal. Contudo, se antecipa a confirmação de que o titular de dados não é indene de responsabilidade por esta mesma situação, mas corresponsável.

Assim, se constatará, potencialmente, o despreparo por parte do Poder Judiciário em garantir a efetiva aplicação das causas excludentes de ilicitude, devido à falta de cuidados (negligência, imprudência) pela vítima - o que ao invés de contribuir para a solução do problema, cria novos dois. De um lado, (i) as pessoas não se sentem motivadas e incentivadas a aprender a se proteger no ciberespaço e de outro, (ii) surge novo “nicho” para acionamento judicial, com a criação de possível indústria do dano moral “LGPD” (por estímulo dos magistrados que, inadvertidamente, aplicam à proteção de dados a mesma lógica do CDC, sem diferenciar as particularidades de cada matéria).

Do cenário que se delinea no horizonte é possível inferir, desde já, a importância do letramento digital de jurisdicionados e do próprio Judiciário como medida preventiva que bloqueará tanto as infrações cometidas a partir de roubo de identidade digital, como a criação de um grande problema de política judiciária.

2. A CIBERIDENTIDADE E OS RISCOS DA ERA DIGITAL.

2.1. ONDE TUDO COMEÇA: A TUTELA DA CIBERIDENTIDADE COMO COROLÁRIO DO PRINCÍPIO DA DIGNIDADE HUMANA E DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

O surgimento da Sociedade da Informação se deu em meados do século XX com o desenvolvimento dos meios de comunicação – cinema, televisão e rádio – atingindo o auge com o estabelecimento da Internet. Daí por diante se instituiu a *Era Digital*, que se consagrou como paradigma à redefinição dos conceitos de territorialidade, tempo, espaço e até mesmo soberania. É o que explica Cancelier:

Tal cenário começa a alterar-se de forma mais contundente no decorrer da década de 1960 motivado, sobretudo, pelo crescimento da circulação de informações, consequência do desenvolvimento exponencial da tecnologia de coleta e sensoriamento [...]¹⁷.

Essa conjuntura, como era de se esperar, impactou fortemente os indivíduos, especialmente quando consideramos que o motor por trás da novidadeira realidade é movido pelo tratamento de dados pessoais.

Coletar informações sobre qualquer pessoa se tornou extremamente acessível. Basta realizar uma busca simples em um mecanismo de pesquisa na internet, explorar as redes sociais ou até mesmo conduzir pesquisas mais detalhadas através de empresas especializadas em bancos de dados ou em enriquecimento de informações. As próprias pessoas reúnem dados pessoais e, frequentemente, as convertem em *hiperlinks* prontamente acessíveis por meio de um *QR code* que contenha detalhes de contato, perfis de redes sociais e quaisquer outras informações julgadas pertinentes.

A relação entre a vida offline e online está se estreitando cada vez mais, o que gera mudanças significativas na forma como os direitos individuais, como a privacidade, a honra e a imagem, são compreendidos. Isso implica na necessidade de uma reinterpretação desses direitos, a fim de assegurar uma proteção efetiva das pessoas no mundo digital.

Enquanto a era digital trouxe avanços notáveis, como a redução de distâncias, a otimização da indústria, a criação de novos empreendimentos baseados em ativos intangíveis, a promoção de novas carreiras, a expansão da liberdade de expressão e uma maior acessibilidade à informação, ela também resultou em uma crescente dependência das pessoas em relação a essas tecnologias, além de introduzir novas fragilidades que podem impactar diretamente suas vidas no mundo físico.

Justamente por isso, a compreensão de um direito à proteção de dados tem evoluído de uma simples salvaguarda da privacidade e da intimidade, passando a incluir a noção de um direito individual ao controle de seus próprios dados pessoais, ou seja, o direito à autodeterminação informativa. Isso ocorreu principalmente porque, ao contrário da visão anterior de “informações desprotegidas” livremente acessíveis na internet, esse conjunto de

¹⁷ CANCELIER, Mikhail Vieira de Lorenzi. **O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro**. Sequência, v. 38, p. 219, 2017. Disponível em: <www.scielo.br/pdf/seq/n76/2177-7055-seq-76-00213.pdf>. Acesso em: 22 set. 23.

informações (advindas de dados pessoais) reflete uma extensa representação da identidade humana, tornando essencial uma sólida proteção legal.

Aliás, conforme Laura Schertel Mendes e Gabriel Fonseca explicam, os dados pessoais constituem a representação virtual do indivíduo na sociedade contemporânea:

São as informações extraídas a partir desses dados, que essencialmente formarão a representação virtual do indivíduo na sociedade. Os dados precisam ser processados e organizados para a extração dessas informações. A partir delas, por exemplo, são geradas decisões ou interpretações que podem ampliar ou reduzir as oportunidades do titular no mercado, formatar sua “imagem” perante os setores público e privado, bem como desenvolver sua personalidade dentro da comunidade digital.¹⁸

Nesse mesmo diapasão, contribuindo para o avanço da proteção legal da identidade digital sob a ótica da proteção de dados pessoais, em 10.02.2022, a Emenda Constitucional nº 115 foi aprovada, introduzindo o inciso LXXIX ao artigo 5º, garantindo o “direito à proteção dos dados pessoais, inclusive nos meios digitais”.¹⁹

Por ela, o direito à proteção de dados pessoais sofreu uma ampliação das salvaguardas constitucionais voltadas para a privacidade, a intimidade e o sigilo das comunicações, para então assumir sua própria conformidade como um direito fundamental autônomo e uma garantia independente – a proteção de dados agora abarca um direito à ciberidentidade.

A constitucionalização do tema, corroborada pela expansão exorbitante de cibercrimes durante a pandemia do Covid-19²⁰, retomou o debate acerca da proteção da própria identidade pessoal no âmbito digital nomeadamente porque a abordagem dos delitos informáticos ficou de

¹⁸ MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. *REI - Revista Estudos Institucionais*, 6(2), p. 98. Disponível em: <https://doi.org/10.21783/rei.v6i2.521>. Acesso em: Acesso em 10 set. 2023.

¹⁹ BRASIL. **Emenda Constitucional nº 155 de 10 de fevereiro de 2022**. 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. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em 15 set. 2023.

²⁰ Segundo dados da Kaspersky, em março/2020 houve um aumento de 124% de ataques a dispositivos móveis, crescimento diretamente ligado às mensagens maliciosas circulando no WhatsApp se aproveitando da pandemia. Isso porque, durante a pandemia, a demanda por softwares de videoconferência aumentou muito, principalmente para empresas, escolas e universidades. Com essa nova demanda, certas brechas de segurança clarificaram consequências graves. Esse foi o caso do Zoom, software para Windows que apresentava uma brecha de segurança, o que permitia que crackers invadissem o app e pudessem roubar senhas e credenciais, além de conseguir acesso e executar comandos arbitrários no sistema. Assim, houve vários casos de roubo de informações dos usuários do aplicativo e, além disso, criminosos passaram a realizar o que eles chamaram de zoombombing, que consistia em invadir certas reuniões ou aulas e interrompê-las com imagens pornográficas, racistas ou de conteúdo inapropriado. Disponível em: <https://www.perallis.com/news/aumento-do-cibercrime-em-tempos-de-pandemia-de-home-office#:~:text=Segundo%20dados%20da%20Kaspersky%3A,dom%C3%ADnios%20suspeitos%20relacionados%20%C3%A0%20pandemia>. Acesso em 05 set 23.

fora do escopo da Lei Geral de Proteção de Dados (LGPD), e a legislação de maior preponderância no tema, Lei Carolina Dieckmann, foi aprovada em 2012²¹, dez anos antes da consagração constitucional da proteção de dados pessoais.

Por outro lado, para além de uma expressão do próprio direito à autodeterminação informacional, e enquanto conjunto de características que individualizam uma pessoa, a identidade pessoal constitui uma das manifestações mais relevantes, talvez em vias de se tornar a mais importante, do próprio princípio da dignidade humana.

A dignidade humana, a seu turno, é um princípio que se desmembra em diversas partes, incluindo a identidade genética individual²², o direito fundamental de conhecer e reconhecer a paternidade e a maternidade²³, o direito de conhecer as origens genéticas, e a identidade civil, que abrange o direito ao nome²⁴, um elemento fundamental de identificação e considerado como parte essencial da identidade pessoal.

Embora a Constituição Federal não faça uma referência explícita, é possível defender que o conceito de identidade pessoal, nos limites do que foi tratado anteriormente, como um direito fundamental, também deve abranger a “ciberidentidade”.

²¹ Em meio aos avanços das novas tecnologias e facilitação do acesso às redes sociais, os crimes cibernéticos tiveram um aumento significativo nos últimos anos. Foi, então, que o Legislativo brasileiro viu a necessidade de tipificar crimes cometidos no ambiente virtual. A Lei Carolina Dieckmann foi apresentada em novembro de 2011 e aprovada um ano depois. No âmbito jurídico, no entanto, a aprovação não foi muito bem recebida, uma vez que o projeto de lei não foi, na avaliação de alguns especialistas, amplamente debatido por conta da tramitação em tempo recorde. Para que os crimes cibernéticos sejam combatidos com eficiência, as leis brasileiras devem acompanhar o mesmo ritmo do avanço das novas tecnologias e o conteúdo deve ser muito bem debatido. “O tema é amplo, atual e sempre coerente. Sendo assim, é um assunto que merece estar sempre em debate, com estudos sobre sua aplicação, ampliação e aperfeiçoamento, pois só assim poderá ser considerada mais efetiva para toda sociedade” afirma o advogado Carlos Eduardo Gonçalves, em entrevista ao JOTA. Disponível em: <https://www.jota.info/justica/lei-carolina-dieckmann-completa-10-anos-com-baixa-efetividade-avalia-especialista-02122022>. Acesso em 05 set 23.

²² O direito de conhecer a própria origem genética está estabelecido em nossa legislação por meio da Lei de Adoção de 2009, que protege a identidade como um componente crucial da dignidade humana. Sem ter conhecimento de sua identidade essencial, que inclui sua ascendência e informações genéticas, o indivíduo é privado de uma parte fundamental de sua própria essência.

²³ Severo Hryniewicz e Regina Fiuza Sauwen diante do fenômeno que produz uma parentalidade incerta afirmam: “na impossibilidade de se avaliar com certeza quem fosse o pai, adotava-se, em sentido amplo, o princípio do jurisconsulto romano Papiniano: “*Pater vero is est quem nuptiae demonstrat*” (É verdadeiramente pai aquele que as núpcias indicam), citado no seu *De suis et legitimis heredibus* (Sobre os seus e os legítimos herdeiros). Este princípio é um artifício jurídico, por tratar –se de presunção iuris tantum.” In: HRYNIEWICZ, Severo; SAUWEN, Regina Fiuza. **O Direito “in vitro” da Bioética ao Biodireito**. 3ª edição. Rio de Janeiro: Lumen Iuris Editora, 2008. 254 p.

²⁴ O nome, como meio de distinguir uma pessoa individualmente, possui uma dimensão pública inquestionável, já que é crucial para identificar o indivíduo em grande parte de suas interações sociais, especialmente quando se trata das relações com o governo. Portanto, é uma faceta indispensável da personalidade.

Para Sherry Turkle²⁵, a ciberidentidade é composta por três traços essenciais: a multiplicidade, a invisibilidade e o anonimato. A multiplicidade diz respeito à habilidade de cada usuário criar várias *personas* online, em contraste com o mundo físico, onde normalmente temos apenas uma identidade. A invisibilidade, que complementa a multiplicidade, permite ocultar ou adicionar características que não correspondem à nossa identidade real. Por último, o anonimato, como o próprio nome indica, possibilita que o usuário navegue online sem revelar sua identidade.

Porém, apesar de a multiplicidade, invisibilidade e anonimato serem características da presença humana na internet, resultantes do funcionamento dos sistemas de computação, não são necessariamente elementos que compõem a ciberidentidade, no âmbito jurídico. Voltando ao objeto da presente análise, por exemplo, não parece que possa ser considerado passível de usurpação para fins legais já que, conforme preceitua Carneiro da Silva “a ciberidentidade enquanto bem jurídico eminentemente pessoal suscetível de usurpação, tem necessariamente que refletir a identidade de uma pessoa humana a ponto de ser possível identificá-la”.²⁶

A interpretação ora adotada, portanto, é de que os dados a serem protegidos devem se referir apenas a “pessoa natural identificada ou identificável”²⁷. Inobstante a isso, como bem destaca Eva Reis²⁸, a proteção constitucional não deve se restringir apenas à “identidade real” (leia-se física). Com efeito, dados puramente eletrônicos podem ser relacionados a uma pessoa identificada ou identificável, como o e-mail pessoal, os perfis em redes sociais como Facebook, TikTok, Instagram e “X” (anteriormente, Twitter), além das informações de acesso à página de *homebanking*, avatares, personagens (de videogame), entre outros exemplos.

Esses dados, embora inexistentes no passado, agora integram a vida cotidiana e a identidade humanas. O uso inadequado deles pode ser tão ou até mais prejudicial do que a divulgação de informações como o número de identidade ou a carteira de motorista. Eles representam uma extensão digital de nossa identidade real, justificando, assim, que sejam tratados com a mesma proteção constitucional concedida à nossa identidade convencional, não

²⁵ TURKLE, Sherry. **Life on the screen: identity in the age of the internet**. London, Weidenfeld & Nicholson, 1996. 352 p.

²⁶ CARNEIRO DA SILVA, Flávio Manuel. **A usurpação da ciberidentidade**. Dissertação de Mestrado — Universidade Católica Portuguesa. 2004. p.16.

²⁷ Assim como na Lei Geral de Proteção de Dados, o dado pessoal constitui “informação relacionada a uma pessoa natural identificada ou identificável”.

²⁸ REIS, Eva da Silva Rodrigues Pinto dos. **Apropriação Indevida de identidade**: enquadramento jurídico-penal. Dissertação de Mestrado – Universidade de Lisboa: Faculdade de Direito, 2019. p. 14.

apenas por uma questão de compatibilidade jurídica (com as normas vigentes), mas também por uma questão de coerência e dialógica das fontes.

Com base nesse conceito de identidade, que inclui a dimensão da ciberidentidade mencionada anteriormente como um direito e garantia fundamental protegido pela Constituição Federal, delimitam-se os parâmetros de análise da proteção à identidade digital que serão abordados ao longo deste trabalho.

No entanto, antes de entrar especificamente nas definições e na relevância de discutir sobre “usurpação de identidade”, é pertinente refletir sobre o comportamento humano no contexto da “sociedade de riscos” – teorizada antes mesmo da Era Digital. Desta forma se compreenderá qual o papel do titular de dados pessoais como primeira linha de defesa na mitigação dos riscos inerentes às rápidas transformações trazidas pela tecnologia na sociedade algorítmica.

2.2. A COMPREENSÃO DA ERA DIGITAL NO CONTEXTO DA SOCIEDADE DE RISCOS

Os crimes e ilícitos cibernéticos, de modo geral, ainda são pouco abordados na legislação brasileira. E sem esperar pelo legislador, estão se tornando mais proeminentes à medida que a tecnologia avança, como uma consequência direta desse avanço. Para uma compreensão mais aprofundada do fenômeno, recorrer-se-á às conclusões de diversos estudiosos, incluindo o sociólogo alemão Ulrich Beck, cujas obras propõem uma análise sociocultural com base na perspectiva do cosmopolitismo, enfatizando especialmente as conexões do mundo contemporâneo.

A percepção do papel da tecnologia na sociedade passou por mudanças desde os primórdios da Revolução Industrial. Nessa época, a tecnologia era geralmente vista de maneira otimista, embora existissem preocupações sobre seu possível impacto na perda de empregos. Era considerada como uma força impulsionadora do progresso e do desenvolvimento social, aliviando as pessoas de trabalhos árduos e sendo vista como uma ferramenta para a emancipação e a promoção da felicidade.

No entanto, após a Segunda Guerra Mundial, surgiram movimentos críticos e céticos em relação ao papel da tecnologia, não necessariamente contra a tecnologia em si, mas questionando suas formas de uso e sua desconexão dos benefícios reais para a humanidade. É

dentro desse contexto ambíguo que este trabalho pretende analisar os riscos associados à tecnologia e investigar como eles afetam a compreensão dos crimes cibernéticos.

Nas interações sociais cotidianas, os riscos cresceram na mesma proporção do desenvolvimento da tecnologia²⁹. Em nossas vidas, com frequência nos deparamos com perigos e ameaças imprevisíveis. Criações originalmente concebidas com o intuito de resguardar a segurança e aprimorar a proteção de bens e indivíduos podem, eventualmente, resultar em consequências indesejadas, transformando-se em novos desafios.

À medida que nossa compreensão evoluiu, a avaliação da relação entre custos e benefícios de determinados riscos se modificou. O que é atualmente considerado um risco aceitável pode, em um futuro próximo, ser amplamente rejeitado pela sociedade.

Nesse contexto, ao analisar as mudanças decorrentes da crescente influência da cibercultura, Spencer Sidow³⁰ identifica alguns dos riscos associados a este cenário. Em primeiro lugar, o autor ressalta que a Internet introduziu a todos os usuários o conceito fundamental do Princípio da Igualdade, que preconiza tratar igualmente os iguais e desigualmente os desiguais.

Para Spencer, na esfera da interação virtual, a segunda parte desse princípio não se aplica. Ele argumenta que não existem disparidades na anonimidade virtual. Tanto um milionário quanto um assalariado têm acesso ao mesmo site, visualizam as mesmas informações e buscam dados em igualdade de condições. Todos podem se destacar com base em méritos e habilidades, independentemente de sua origem. Portanto, todos coexistem no mesmo ambiente, sem discriminação aparente.

Contudo, Sidow destaca uma lacuna significativa nessa representação: embora a internet *teoricamente*³¹ possa operar como uma meritocracia onde todos têm igualdade de

²⁹ GIDDENS, Anthony. **O mundo na era da globalização**. Lisboa: Editorial Presença, 2000. 48 p.

³⁰ SYDOW, Spencer Toth. **Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática**. Orientador: Sergio Salomão Shecaira. 2009. Dissertação (Mestrado no curso de Direito) - Universidade de São Paulo, São Paulo, 2009. 162 p.

³¹ Vê-se, contudo, que nas redes sociais o sistema tende a não funcionar de forma completamente igualitária e objetiva. Basta observar que o Facebook, por exemplo, utiliza um programa chamado “XCheck” (verificação cruzada), que permite a celebridades, políticos e outros membros da elite estadunidense tratamento diferenciado em relação a algumas políticas de moderação de conteúdo que usuários comuns precisariam respeitar. O acesso em contas “verificadas” também é diferenciado. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/facebook-reformula-processo-de-moderacao-de-conteudo-para-vips/>. Acesso em: 20 nov. 23

oportunidades, o acesso ao poder online está intrinsecamente vinculado ao conhecimento da linguagem e à compreensão da manipulação de dados.

Uma pessoa de destaque na sociedade offline, se não tiver conhecimento sobre os detalhes da manipulação de informações e programação, se torna simplesmente um usuário comum na internet. Por outro lado, um indivíduo comum, mas com habilidades nessa área, pode fazer parte de uma elite cibernética.

Contudo, a transferência de poder (por meio da informação) para aqueles que têm conhecimento da linguagem e dos procedimentos levou a abusos na internet. O aumento da relevância das informações convertidas em *bits*, impulsionado pela indispensabilidade da rede, deu aos dados um valor econômico significativo. À medida que o ambiente virtual cresce em influência e substitui aspectos da vida cotidiana, novos dados são constantemente gerados e almejados. Isso, por sua vez, faz com que a internet se torne um alvo para a cultura criminosa.

Essa perspectiva se alinha de maneira precisa com a ideia subjacente à concepção de uma sociedade global permeada por riscos. Na óptica de Ulrich Beck³², o avanço da ciência e da tecnologia impulsionou o crescimento econômico das sociedades ocidentais, mas, simultaneamente, deu origem a novas categorias de ameaças. Na visão de Beck, o risco emergiu como uma característica essencial das sociedades modernas, levando-o a caracterizá-las como "sociedades de risco".

A ideia de sociedade de risco emerge como uma reação à inadequação da sociedade industrial, na qual também se nota a deterioração de certas funções sociais³³. Essa terminologia está principalmente ligada a um traço das sociedades modernas, onde os riscos sociais, pessoais, políticos e econômicos estão progressivamente escapando da capacidade de proteção, regulação e supervisão que predominavam na sociedade industrial.

No início do século XXI, com o avanço da era digital e a consequente interconexão global proporcionada pelas tecnologias de comunicação, os perigos e riscos gerados pela sociedade transcenderam fronteiras étnicas ou religiosas³⁴. Os riscos, agora globais, passaram a se caracterizar pela sua deslocalização, imprevisibilidade e incompensabilidade. A deslocalização se refere ao fato de que suas causas e consequências não estão restritas a uma

³² BECK, Ulrich. **Risk society. Towards a new modernity**. Londres: Sage, 1992. 272 p.

³³ BECK, Ulrich; GIDDENS, Anthony.; LASH, Scott. **Modernização reflexiva: Política, tradição e estética na ordem social moderna**. Oeiras: Celta Editora, 2000.

³⁴ BECK, Ulrich; GIDDENS, Anthony.; LASH, Scott. **Modernização reflexiva: Política, tradição e estética na ordem social moderna**. Oeiras: Celta Editora, 2000. p.27.

região geográfica específica, espalhando-se rapidamente pelo mundo, com efeitos de longo prazo. A imprevisibilidade consistiria no caráter hipotético desses riscos, cujas consequências são inicialmente incalculáveis. A incomensurabilidade ocorre porque não é mais possível anular os danos causados por esses riscos nocivos.³⁵

A teoria evolui. Beck argumenta que a nova sociedade reconhece que está constantemente exposta a riscos e possui a habilidade de identificá-los e, conseqüentemente, lidar com eles.

Assim, o progresso tecnológico levou a humanidade a criar tecnologias, ao mesmo tempo em que nos permitiu identificar os perigos decorrentes desses avanços. Isso nos capacita a adotar medidas para evitar ameaças desnecessárias e controlar comportamentos que poderiam aumentar a quantidade mínima de riscos aceitáveis no processo de evolução social.

Como dito anteriormente, a rede mundial trouxe uma aceleração nas interações (sejam elas comerciais, sociais, internacionais, etc.) e eliminou as barreiras físicas, possibilitando aos usuários uma sensação de liberdade como nunca antes experimentada.

Impulsionada pela empolgação com essa nova ferramenta, a sociedade adotou rapidamente as práticas oferecidas pela informática, adquirindo computadores e celulares em grande escala e adotando amplamente a tecnologia. Por outro lado, é evidente que, quando se trata da sociedade da informação, a compreensão dos riscos ainda não foi completamente internalizada.

Grande parte desta incompreensão se dá justamente porque o uso da tecnologia se opera como um verdadeiro *trade-off* tentador: metaforicamente pode ser comparado a um "veneno" que, ao mesmo tempo, contém o "antídoto" para certos problemas contemporâneos.

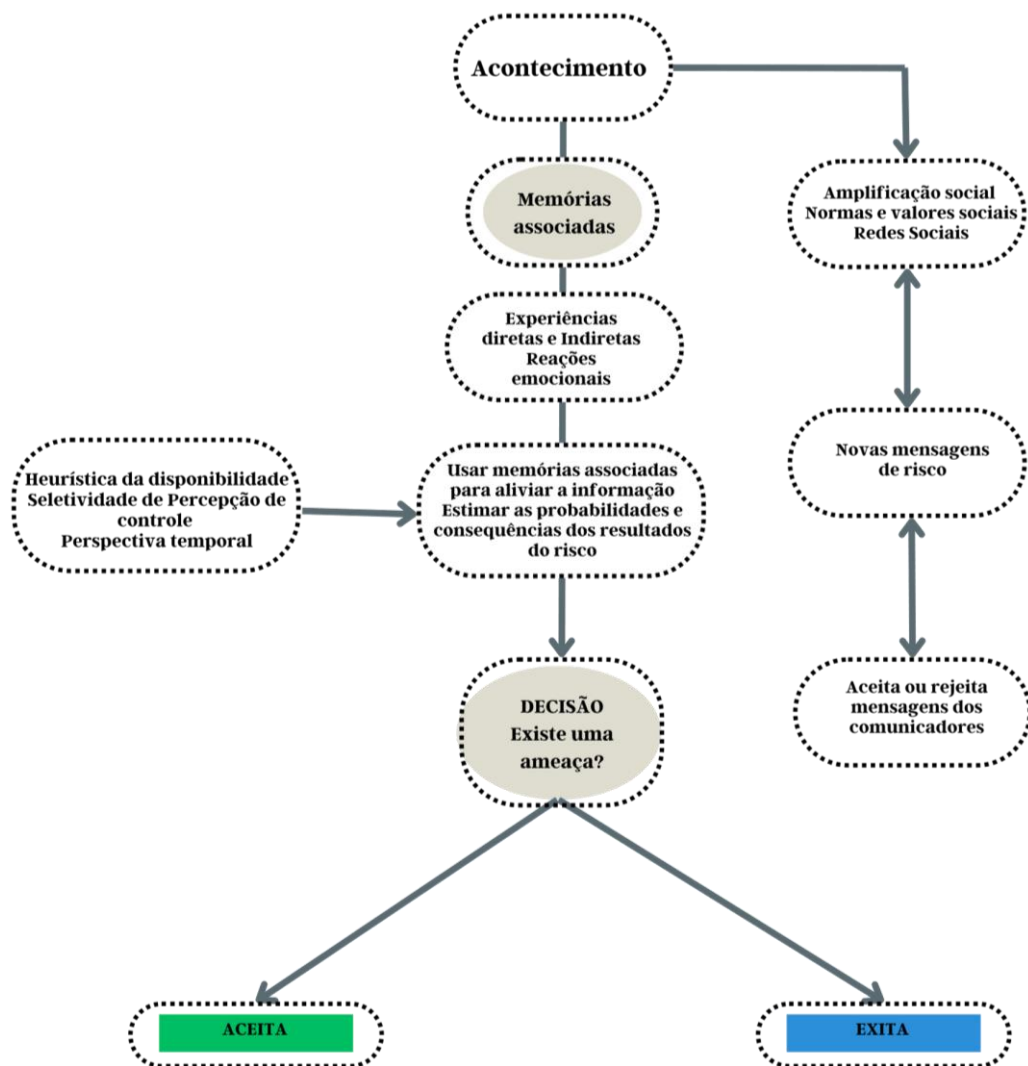
Não obstante, para Fischhoff *et al.*³⁶, os riscos associados às tecnologias modernas não podem ser considerados apenas sob a perspectiva das consequências negativas que podem gerar, uma vez que ninguém produziria e até mesmo investiria em tecnologias se elas não proporcionassem benefícios a alguém. Ao optar por adotar uma tecnologia específica, precisamos aceitar o conjunto de características que ela traz consigo, incluindo tanto os benefícios quanto os possíveis prejuízos, pois ambos estão intrinsecamente ligados.

³⁵ BECK, Ulrich; GIDDENS, Anthony.; LASH, Scott. **Modernização reflexiva: Política, tradição e estética na ordem social moderna**. Oeiras: Celta Editora, 2000. p.94.

³⁶ FISCHHOFF, Baruch; WATSON, Stephen R; HOPE, Chris. **Defining risk, Policy Sciences**, 1984, n.º 17, pp. 123-139.

Não se pode olvidar que as pessoas constroem percepções próprias sobre os riscos e, em grande parte, é a partir dessas impressões pessoais que tomam decisões sobre aceitá-los ou não. Eiser³⁷ desenvolveu um fluxograma simplificado que explora alguns dos fatores que influenciam o julgamento do público diante de cenários de risco ou ameaça. Nessa representação abaixo reproduzida (Figura 2), além das dimensões sociais, estão incorporadas as experiências individuais de cada pessoa.

Figura 1: Processo de julgamento público do risco



Fonte: Adaptado de Eiser (2004, p.40)

³⁷ EISER, J. Richard. **Public perception of risk**. UK: Report prepared for Foresight, Office of Science and Technology, 2004. pp. 52–63. Disponível em: <http://www.jstor.org/stable/41376908>. Acesso em: 20 set. 2023.

De acordo com Douglas e Wildavsky³⁸, geralmente os diversos membros da sociedade estabelecem uma distinção clara entre os riscos que eles escolhem assumir voluntariamente e aqueles que são impostos a eles. Os riscos que são involuntariamente impostos tendem a ser mais propensos a rejeição pelo público em comparação com aqueles que são aceitos voluntariamente. Além disso, um ponto importante abordado por esses autores é a indicação de que a distribuição dos riscos na sociedade não ocorre de forma uniforme.

Certos segmentos ou estratos da sociedade enfrentam níveis mais elevados de risco do que outros. Os autores ilustram essa situação da seguinte forma: em média, as pessoas com menor poder econômico tendem a ter pior saúde do que aquelas mais ricas, apresentam uma expectativa de vida mais curta e estão sujeitas a um maior número de acidentes. No entanto, não se pode argumentar que essas pessoas, ao enfrentarem níveis mais altos de risco em suas vidas, o façam de forma voluntária.

Em relação a determinados tipos de riscos, a relação entre os custos suportados e os benefícios esperados desempenha um papel crucial nas decisões tomadas. É natural que algumas pessoas prefiram se expor a riscos no ambiente de trabalho ou no ambiente em que vivem em vez de ficarem desempregadas.

Quando essas opções são avaliadas, como a escolha entre manter o emprego (e enfrentar riscos ocupacionais) ou deixar o emprego (e evitar os riscos associados a ele), é instintivo que se opte por manter o emprego. O trabalho representa a principal fonte de sustento para a grande maioria da população global³⁹.

Portanto, existem influências sociais específicas, incluindo aquelas coercivas, que afetam a aceitação do risco (por exemplo, a necessidade de aceitar determinados riscos para manter o emprego, o que, por sua vez, permite sustentar os filhos). É verdade que alguns tipos de riscos podem não ser desejados, mas as pessoas precisam tomar decisões, especialmente quando se trata de ponderar os custos e benefícios para aspectos importantes de suas vidas.

Além disso, é importante considerar que a identificação e a avaliação subestimada ou superestimada de determinados riscos não ocorrem em um vácuo social; ao contrário, podem

³⁸ DOUGLAS, Maria. e WILDAVSKY, Aaron. **Risk and culture: An essay on the selection of technological and environmental dangers**. Berkeley (CA): University of California Press, 1982. Disponível em: <https://www.jstor.org/stable/10.1525/j.ctt7zw3mr>. Acesso em: 20 set. 2023.

³⁹ ANTUNES, Ricardo. **Desenhando a nova morfologia do trabalho**: As múltiplas formas de degradação do trabalho. Revista Crítica de Ciências Sociais (Coimbra), 2008, n.º 83, pp. 19-34. Disponível em: <https://doi.org/10.4000/rccs.431>. Acesso em 10 set. 2023.

ser moldadas por diversos campos do conhecimento científico ou conhecimento comum, por interesses estabelecidos, por fatores econômicos ou políticos, por diferentes avaliações sociais (que podem ser influenciadas, por exemplo, pela associação a grupos sociais específicos), por competições pelo controle de recursos específicos, por estratégias organizacionais ou institucionais, e assim por diante.

Assim, é possível compreender que a definição do que pode ser considerado como um risco no contexto social está se tornando cada vez menos objetiva e cada vez mais um fenômeno vulnerável a várias interpretações, interesses e subjetividades.

Isso explica, por exemplo, porque no contexto de sociedade datificada mesmo o usuário tendo as informações dos riscos que o uso de certas aplicações de internet traz ao titular de dados – como aplicativos que promovem *trends* na internet com manipulação de imagens, mas que em contrapartida promovem o tratamento de dados a longo prazo – continua a utilizá-las. Ora, mesmo o uso de inofensivos e-mails e buscadores gratuitos está inerentemente vinculado a risco de perfilhação e monitoramento, manipulação e monetização de dados pessoais.

É importante considerar que muitos dos riscos na sociedade virtual são abstratos, assim como o próprio meio, e, portanto, são mais difíceis de serem percebidos pelos cidadãos virtuais. O escudo representado pela tela do computador muitas vezes proporciona ao usuário uma sensação de segurança, criando a ilusão de invulnerabilidade. Ao não estar exposto às suas fragilidades, prevalece a ideia de segurança, e as pessoas tendem a agir com menos restrições e mais audácia nessas circunstâncias.

Essa figura se torna especialmente relevante na maneira como os internautas conduzem sua navegação na internet. Quando se sentem protegidos ou não percebem que têm algo a perder, os usuários comuns tendem a agir com menos cuidado, navegando em sites de forma negligente e perdendo a cautela ao abrir e-mails de remetentes desconhecidos ou clicar em anexos, entre outras ações.

Além disso, a dificuldade que os usuários enfrentam ao compreender o valor das informações geradas no ambiente virtual contribui para criar as condições ideais para comportamentos criminosos. Dessa forma, a maioria esmagadora dos internautas navega em endereços online sem conseguir avaliar com precisão o nível de segurança e a necessidade de prudência ao permanecer nesses sites.

O ponto a ser destacado nesta sociedade de risco é que, enquanto a tecnologia proporciona aos usuários uma ampla liberdade e igualdade individual, ela também reduz a

capacidade de distinguir as pessoas com as quais se relacionam virtualmente além de limitar a sensação de segurança, tornando-a uma ideia distante da realidade.

É importante considerar que a própria natureza da internet torna a vítima vulnerável e desempenha um papel significativo em comportamentos criminosos. Contudo, a web é um ambiente para o qual a vítima muitas vezes deseja retornar, seja por necessidade seja por interesse, uma vez que simplesmente abandonar essa ferramenta de integração social é quase que impossível.

Na realidade, alguns dos riscos atuais parecem assumir uma espécie de efeito *boomerang*, isto é, metaforicamente, aqueles que introduzem o risco também correm o risco de se tornarem suas potenciais vítimas.

Justamente por isso, cabe também à vítima compreender a sociedade de risco na qual ela e o infrator estão inseridos, reconhecendo que sua postura e conduta nesse contexto devem ser muito mais cautelosas e conscientes. Os riscos avaliados, nesse caso, são coletivos e representam o cuidado necessário para manter a convivência harmoniosa. Navegar no escuro exige atenção redobrada, passos cuidadosos e o uso de outros mecanismos de orientação além da visão.

Porém, apesar de haver uma variedade de riscos envolvidos, é comum que os usuários da Internet não reconheçam que este ambiente é, em essência, uma extensão da sociedade. Essa expansão traz consigo alguns dos mesmos riscos encontrados na sociedade física, bem como riscos novos originados das características facilitadoras e da alta velocidade da Internet. Por exemplo, Spencer destaca como é fácil verificar que um cidadão comum costumeiramente toma precauções para não interagir com estranhos na vida real, mas geralmente não adota a mesma cautela no ambiente virtual, onde a comunicação com desconhecidos é frequentemente aceita com simpatia e surpresa.⁴⁰

Em resumo, a realidade virtual criada pela tecnologia da informação muitas vezes se assemelha, em vários aspectos, à vida cotidiana. Logo, respeitadas as premissas fáticas, assim como as pessoas são ensinadas desde a infância a não conversar com estranhos no mundo real, o mesmo princípio pode ser aplicado ao ambiente virtual, onde a visita a sites desconhecidos também requer cautela e cuidado.

⁴⁰ SYDOW, Spencer Toth. **Delitos informáticos próprios**: uma abordagem sob a perspectiva vitimodogmática. Orientador: Sergio Salomão Shecaira. 2009. Dissertação (Mestrado no curso de Direito) - Universidade de São Paulo, São Paulo, 2009. p.36.

O avanço contínuo da tecnologia requer uma reflexão mais profunda, por parte dos indivíduos, sobre suas possíveis repercussões negativas, além dos benefícios que oferece, incluindo os tipos de acidentes que pode desencadear. É fundamental lembrar que os acidentes são uma característica inerente ao universo⁴¹.

As tecnologias incorporam incertezas mal compreendidas que estão fora de nosso controle, especialmente em suas interações com o sistema social. No entanto, parece que ainda estamos longe de reconhecer essa realidade com a devida humildade e seriedade⁴².

A presença ubíqua de riscos tecnológicos em sistemas complexos, em grande parte, serve como prelúdio para acidentes⁴³. Não há organizações imunes ao risco, o que implica que acidentes são eventos inevitáveis e podem ocorrer a qualquer momento.

No entanto, isso não significa que a prevenção seja inútil, mas é relevante entender que mesmo a estratégia de prevenção mais eficaz possui suas limitações. De acordo com Perrow⁴⁴, organizações que operam sistemas tecnológicos complexos ou ultracomplexos já demonstraram que não podem eliminar todos os acidentes.

Essa situação não necessariamente indica que se está lidando com organizações incompetentes ou incapazes de controlar os riscos de suas atividades. Em vez disso, revela principalmente que a segurança na web possui limitações inerentes à sua própria natureza. Além disso, muitas vezes as pessoas ignoram a própria falta de conhecimento, o que pode se tornar perigoso.

É inegável que as tecnologias geralmente oferecem benefícios e riscos (esse aspecto é amplamente aceito). O que se torna complexo e problemático no debate sobre algumas tecnologias é a decisão política de aceitá-las ou rejeitá-las. É crucial avaliar se, com base nessa nova sociedade, um agente aumentou ou criou riscos toleráveis pela sociedade e, ao fazê-lo, concretizou esses riscos de acordo com as normas existentes ou com normas que possam reger novos interesses jurídicos.

A análise da tutela jurídica da vítima de crimes cibernéticos, portanto, requer uma compreensão completa do contexto social em que esta vítima está inserida e, sobretudo, a

⁴¹ GREEN, Judith. **Risk and misfortune: The social construction of accidents**. Londres: Routledge, 1997. 232p.

⁴² BECK, Ulrich. **Risk society. Towards a new modernity**. Londres: Sage, 1992.

⁴³ AREOSA João. Do risco ao acidente: Que possibilidades para a prevenção? Luanda: **Revista Angolana de Sociologia**, 2009, n.º 4, pp. 39-65.

⁴⁴ PERROW, Charles. **Normal accidents: living with high-risk technologies**. New Jersey: Princeton University Press, 1999. 464 p.

relevância do seu dever de cautela na sociedade de riscos mundial. De toda sorte, é impossível analisar tais considerações sem ter uma compreensão clara do conceito de cibercrime, como a doutrina o classifica, suas principais modalidades, quais interesses jurídicos ainda precisam de definição e proteção, e quem está envolvido direta ou indiretamente nessa nova tendência social.

2.2.1. Fraudes na Sociedade de Dados e da Informação

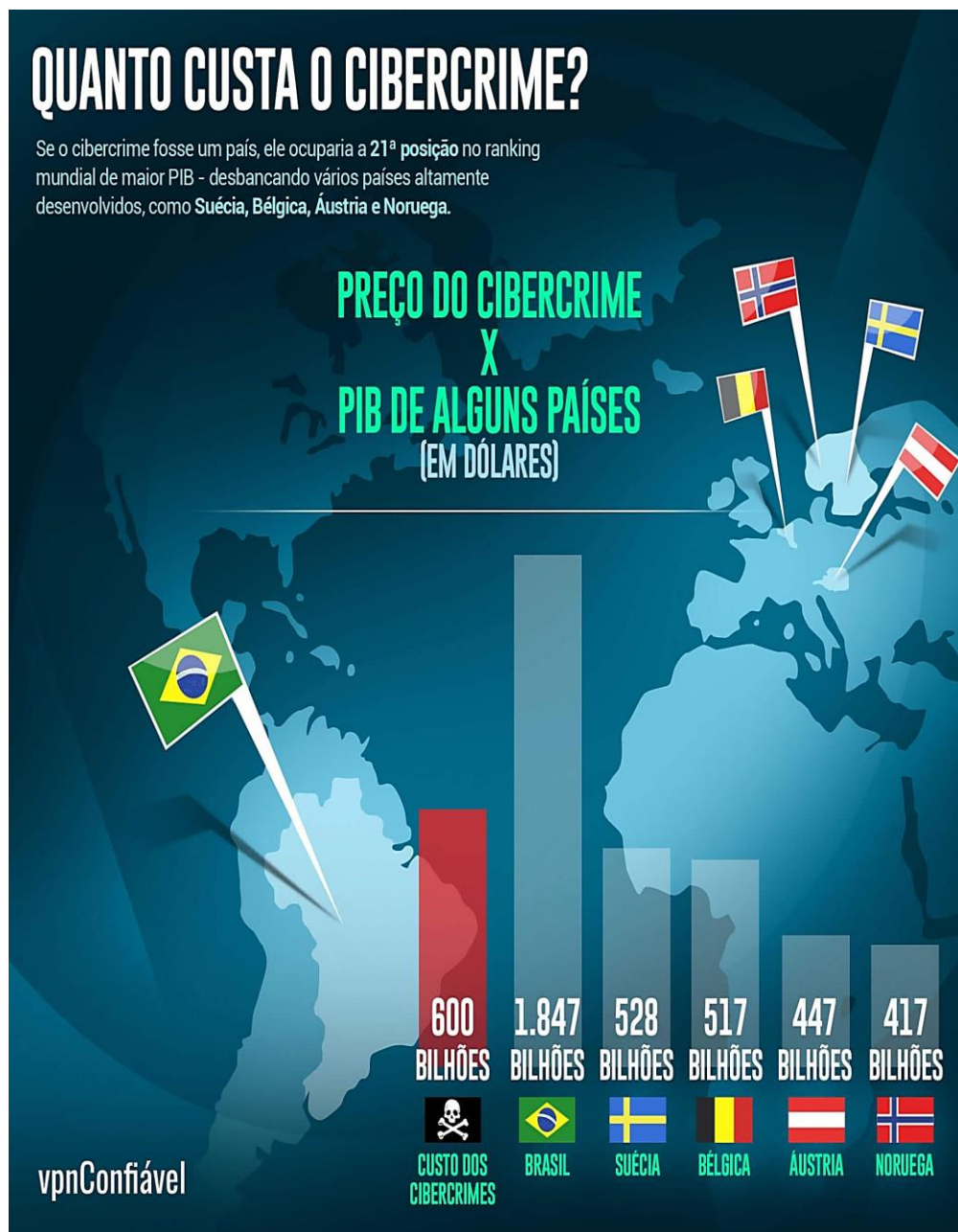
De acordo com o relatório da Apura Cyber Intelligence, as ameaças digitais relacionadas a fraudes financeiras no Brasil experimentaram um aumento significativo durante o primeiro semestre de 2022. Especificamente, o número de tentativas de fraude online envolvendo cartões cresceu em impressionantes 637% em comparação com o mesmo período do ano anterior.⁴⁵

No que diz respeito às implicações financeiras dos delitos cibernéticos, uma pesquisa realizada pelo Centro de Estudos Estratégicos e Internacionais em parceria com a *McAfee* calculou que o impacto anual global alcança a marca de 600 bilhões de dólares, o que corresponde a cerca de 0,8% do Produto Interno Bruto (PIB) global. O Brasil, por sua vez, contribui com pelo menos 10 bilhões de dólares desse total.

Para ilustrar essa dimensão financeira, o custo dessas perdas equivale a quase um terço do PIB brasileiro e colocaria o país na 21ª posição no ranking do Produto Interno Bruto do mundo, de acordo com o Fundo Monetário Internacional. Isso o posicionaria à frente de nações como Suécia, Bélgica, Áustria e Noruega em termos de tamanho da economia.

⁴⁵ Disponível em: <https://forbes.com.br/forbes-money/2022/09/cibercrime-tentativas-de-fraudes-financeiras-crescem-no-brasil/>. Acesso em: 15 set. 23

Figura 2: Quanto custa o cibercrime?



Fonte: Centro de Estudos Estratégicos e Internacionais em parceria com a McAfee. Reprodução de: VPN Confiável fala sobre crime cibernético no Brasil⁴⁶

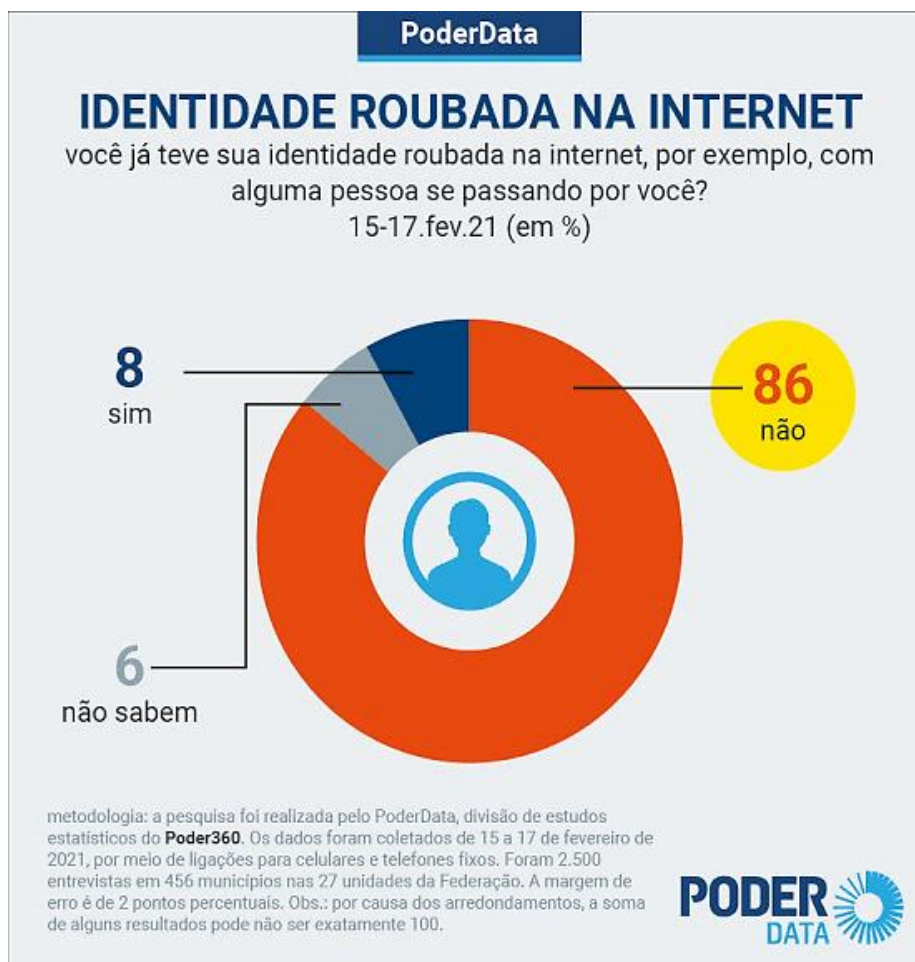
Segundo estudo conduzido pelo PoderData⁴⁷, 8% da população brasileira teve sua identidade virtual roubada. Esse levantamento foi realizado entre os dias 15 e 17 de fevereiro

⁴⁶ Disponível em: <https://www.vpnconfiavel.com/blog/crime-cibernetico-no-brasil>. Acesso em: 15 set. 23.

⁴⁷ Disponível em: <https://www.poder360.com.br/pesquisas/8-tiveram-identidade-roubada-na-internet-mostra-poderdata/>. Acesso em: 15 set. 23.

de 2021 e envolveu a participação de 2.500 indivíduos em 456 municípios localizados nas 27 unidades federativas do país.

Figura 3: Pesquisa sobre “roubo” de identidade na internet



Fonte: Poder Data. Reprodução de: 8% tiveram identidade roubada na internet⁴⁸.

Além disso, a pesquisa proporcionou análises específicas considerando variáveis como gênero, faixa etária, localização geográfica, nível de escolaridade e renda.

⁴⁸ Disponível em: <https://www.poder360.com.br/pesquisas/8-tiveram-identidade-roubada-na-internet-mostra-poderdata/#:~:text=Pesquisa%20PoderData%20indica%20que%208,de%20telefone%2C%20CPF%20e%20endere%20C3%A7o>. Acesso em: 15 set. 2023.

Figura 4: Pesquisa por estratificação - Identidade roubada internet



Fonte: Poder Data. Reprodução de: 8% tiveram identidade roubada na internet⁴⁹.

⁴⁹ Disponível em: <https://www.poder360.com.br/pesquisas/8-tiveram-identidade-roubada-na-internet-mostra-poderdata/#:~:text=Pesquisa%20PoderData%20indica%20que%208,de%20telefone%2C%20CPF%20e%20endere%20C3%A7o.> Acesso em: 15 set. 2023.

A facilitação do anonimato no ciberespaço possibilita que os usuários convivam e interajam com terceiros sem garantias sobre quem eles são na vida real. Para mitigar essa incerteza, os ambientes online costumam implementar sistemas de identificação presumida.

No entanto, a implementação desses sistemas não está isenta de desafios. Questões relacionadas à privacidade, segurança e confiabilidade das plataformas podem surgir, exigindo um equilíbrio delicado entre a proteção dos usuários e a preservação de sua liberdade e privacidade. Portanto, a evolução contínua desses mecanismos é crucial para adaptar-se às demandas em constante mudança do ciberespaço, garantindo um ambiente virtual seguro e ao mesmo tempo respeitando os direitos individuais dos usuários.

Na sequência, analisaremos a usurpação da identidade enquanto mecanismo viabilizador da fraude. Esse fenômeno, como se viu, transcende os limites físicos e ganha contornos acentuados no ambiente digital, onde a facilidade de manipular informações e a dificuldade de identificação do agente conferida pelo anonimato contribuem para sua proliferação.

2.3. A USURPAÇÃO DE IDENTIDADE COMO UM PROCESSO DE DUAS ETAPAS

Antes de iniciar uma investigação sobre a usurpação de identidade, é fundamental definir de maneira precisa a hipótese, suas características distintivas, bem como a forma de classificá-la e os bens jurídicos em questão.

Os delitos cibernéticos podem ser categorizados em várias classes, incluindo invasão de sistemas, fraudes, “roubo” de identidade, pirataria, pornografia online e cyberbullying. No Brasil, a primeira legislação relacionada a esses delitos foi estabelecida em 2012, com um foco principalmente voltado para os aspectos físicos desses crimes. Portanto, para que um ato seja considerado um crime cibernético, ele deve envolver a violação dos direitos da vítima, como a invasão de dispositivos de informática, falsificação de documentos pessoais, clonagem de cartões ou a interrupção ou perturbação de serviços de comunicação, sejam eles telegráficos, telefônicos, informáticos, telemáticos ou de utilidade pública.⁵⁰

⁵⁰ BRASIL, **Lei nº 12.737**, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm. Acesso em 20 set 2023.

E embora o Brasil tenha aderido à Convenção do Conselho da Europa contra a Criminalidade Cibernética, que visa fortalecer a proteção de dados e da dignidade humana, ainda persiste uma certa falta de rigor no tratamento dos crimes virtuais.

Em 2014, foi promulgado o Marco Civil da Internet, que definiu os termos do mundo virtual, suas práticas legais e estabeleceu medidas de proteção e direitos relacionados à privacidade online, essenciais para assegurar o acesso pleno ao ambiente virtual.⁵¹

A Lei 12.965 de 2014, popularmente conhecida como Marco Civil da Internet (MCI), reconhece a importância do acesso à internet para o exercício da cidadania e, por isso, estabelece princípios, garantias, direitos e responsabilidades para a utilização da internet no Brasil. A elaboração do MCI teve como propósito preencher as lacunas no sistema jurídico referentes aos crimes cometidos no cenário virtual⁵².

Optamos, neste trabalho, pelo termo "usurpação de identidade" para descrever a prática de utilizar informações pessoais de outra pessoa com a intenção de se passar por ela perante terceiros. No entanto, é importante notar que essa prática pode ser designada por diversos termos, dependendo das preferências dos pesquisadores de diferentes áreas ou das escolhas do legislador em outros sistemas jurídicos.

Nos Estados Unidos e no Reino Unido, tanto a doutrina⁵³ quanto a lei⁵⁴ fazem uso dos termos "*identity theft*" e "*identity fraud*," que em tradução literal significam "roubo de identidade" e "fraude de identidade," respectivamente.

A distinção entre os dois fenômenos reside na diferença entre simplesmente "roubar" dados (*identity theft*) e, em uma fase subsequente, usar esses dados em benefício próprio ou de terceiros (*identity fraud*). Essa configuração de fraude é equivalente ao crime de estelionato em nosso sistema jurídico penal. O estelionato, em suas diversas formas, envolve a intenção de obter vantagem ilícita em prejuízo de terceiros, induzindo ou mantendo alguém em erro por

⁵¹ ALVES, Marco Antônio; DINIZ, Thiago Dias de Matos; CASTRO, Viviane Vidigal de. **Criminologia e cybercrimes**. Belo Horizonte: RECAJ – UFMG, 2020.

⁵² OLIVEIRA, Bruna Machado de. *et al.* Crimes virtuais e a legislação brasileira. (Re) **Pensando o Direito. Rev. Do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo**. v. 7, n. 13, 2017. 13 p.

⁵³ Neste sentido: WHITE, Michael D. / FISHER, Christopher - Assessing Our Knowledge of Identity Theft: The Challenges to Effective Prevention and Control Effort; WANG, Wenjie/ YUAN, Yufei/ ARCHER, Norm - A Contextual Framework for Combating Identity Theft; LYNCH, Jennifer - Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks; WALL, David S./ Williams, Mathew L. – **Policing Cybercrime: Networked and Social Media Technologies and the Challenges for Policing**

⁵⁴ Veja-se o "*Identity Theft and Assumption Deterrence Act*" ou o Capítulo 47 (Título 18), do Código dos EUA. Disponível em: <https://www.ftc.gov/legal-library/browse/rules/identity-theft-assumption-deterrence-act-text>. Acesso em: 20 set. 2023.

meio de artifícios, truques ou qualquer outro meio fraudulento (conforme estabelecido no artigo 171 do Código Penal).

A distinção entre os dois termos parece ser útil, uma vez que representa duas fases ou fases autônomas de um tipo. No entanto, para parte da doutrina, essa terminologia não é mais apropriada. Para entender por que isso ocorre, é pertinente analisar alguns tipos legais do nosso Código Penal.

Tanto o furto quanto o roubo se concretizam na subtração de uma coisa móvel, conforme definido nos artigos 155⁵⁵ e 157⁵⁶ do Código Penal. Essa subtração deve ser realizada com a intenção de manter a posse da coisa, ou seja, incorporá-la à sua esfera jurídica ou à de terceiros, sem a devida autorização para fazê-lo.

Ambos os delitos estão contidos nos capítulos I e II do Título II, que trata dos crimes contra o Patrimônio. De se recordar que o patrimônio, protegido pelo Direito Penal no Título II da parte especial do Código Penal, engloba não apenas bens de valor econômico mensurável, mas também aqueles que, mesmo não tendo essa característica, possuem algum valor para seu proprietário ou detentor, pois atendem às suas necessidades, sentimentos, usos ou prazeres⁵⁷.

No mesmo sentido, temos a lúcida opinião de Antolisei. Esclarece o douto penalista italiano que:

*O patrimônio não abrange apenas as relações jurídicas de valor econômico mensurável - ou seja, os direitos que podem ser avaliados em termos monetários - mas também aqueles relacionados a objetos que têm valor sentimental (lembranças de família, objetos de estima especial, etc)*⁵⁸

Essa explicação dos conceitos de furto e roubo tem o objetivo de ressaltar que o termo "roubo de identidade" não é tecnicamente correto, pois a identidade é uma realidade complexa que não pode ser simplesmente retirada de outra pessoa por meio de violência. De fato, a identidade, sendo fundamentalmente informação, não pode ser considerada uma coisa tangível

⁵⁵ **Art. 155** - Subtrair, para si ou para outrem, coisa alheia móvel -**Pena:** reclusão, de um a quatro anos, e multa.

⁵⁶ **Art. 157** - Subtrair coisa móvel alheia, para si ou para outrem, mediante grave ameaça ou violência a pessoa, ou depois de havê-la, por qualquer meio, reduzido à impossibilidade de resistência **Pena:** reclusão, de quatro a dez anos, e multa.

⁵⁷ JOPPERT, Alexandre Couto. O real conceito de patrimônio para o direito penal. Disponível em: <https://jus.com.br/artigos/7370/o-real-conceito-de-patrimonio-para-o-direito-penal>. Acesso em: 15 set. 23.

⁵⁸ ANTOLISEI, Francesco; CONTI, Luigi. **Manuale di diritto penale / [1], Parte generale**. Milano: A. Giuffrè, 2003. p. 189 (tradução própria).

que pode ser entregue, uma entidade física passível de ser subtraída (ou seja, furtada ou roubada).

As leis do México e da Espanha, por outro lado, se referem ao ato como "*usurpación de identidad*", descrevendo de maneira abrangente alguém que se faz passar por outra pessoa, sem fazer distinção entre a fase de obtenção de dados e a fase de apropriação. O termo "usurpação" é utilizado para indicar a discordância em relação ao termo menos preciso "roubo de identidade", pois, como dito, a identidade não pode ser roubada, apenas usada.

Ainda há necessidade de fornecer algumas explicações sobre outro termo frequentemente empregado: fraude de identidade. De acordo com Beals, DeLiema e Deevy⁵⁹, para que ocorra uma fraude, é essencial que três elementos se combinem: 1) o uso de engano, 2) a persuasão e 3) a participação ativa da vítima. Além disso, DeLiema, Mottola e Deevy⁶⁰ acrescentam a necessidade de uma tentativa consciente de convencer a vítima a se envolver em transações que, sem o uso do engano, ela nunca concordaria em realizar.

Com base nessas premissas, alguns pesquisadores destacam que a fraude deve ser considerada como uma forma de crime econômico, pois envolve um "ato intencional que resulta em um benefício econômico (ou na evitação de uma perda) para o fraudador e em uma perda para a vítima"⁶¹.

Num estudo realizado por Kävrestad⁶² se investigou a identificação dos fatores essenciais para definir a fraude online. Conforme a autora, três elementos-chave devem ser considerados: 1) os meios utilizados, ou seja, as ferramentas empregadas para cometer o crime, como se a vítima foi abordada por meio de sites de leilões, e-mails, chamadas telefônicas, etc.; 2) a oportunidade, que se refere à capacidade do infrator de cometer o delito; e 3) o motivo que

⁵⁹ BEALS, Michaela; DELIEMA, Marguerite; DEEVY, Martha. 2015. Framework for a taxonomy of fraud. Financial Fraud Research Center *apud* FONSECA, Ana Catarina Cardoso. **Fraude ao consumidor online: variáveis explicativas da vitimação e reportagem**. 2021. p.7

⁶⁰ DELIEMA, Marguerite; MOTTOLA, Gary; DEEVY, Martha. 2017. Findings from a pilot study to measure financial fraud in the United States. Stanford Center on Longevity Working Paper. February *apud* FONSECA, Ana Catarina Cardoso. **Fraude ao consumidor online: variáveis explicativas da vitimação e reportagem**. 2021. p.7.

⁶¹ KEMP, Steven; MONEVA, Asier. 2020. Fraude online vs. offline: Factores predictores de victimización y su impacto. InDret, 1.2020 *apud* FONSECA, Ana Catarina Cardoso. **Fraude ao consumidor online: variáveis explicativas da vitimação e reportagem**. 2021. p.7.

⁶² KÄVRESTAD, Joakim. 2014. Defining, categorizing and defending against online fraud. University of Skövde *apud* FONSECA, Ana Catarina Cardoso. **Fraude ao consumidor online: variáveis explicativas da vitimação e reportagem**. 2021. p.7.

o levou a realizar a fraude, geralmente envolvendo a busca por lucro, seja financeiro ou não financeiro.

Uma vez que não se pode afirmar com certeza, a partir das hipóteses examinadas neste estudo, se a sociedade algorítmica está diante de um ilícito que exige a participação ativa da vítima, mesmo que essa participação ocorra (de forma não consciente ou não), empregar-se-á o termo "usurpação de identidade".

Configura-se a "usurpação" quando o uso da "identidade" ocorre sem o consentimento do titular. A falta de consentimento é um elemento essencial do tipo e reflete a ideia de que se afetou diretamente o titular dos dados pessoais.

Adotar-se-á a definição inglesa/norte-americana segundo as quais a apropriação indevida de identidade se dá em duas etapas: a obtenção de dados (equivalente ao "roubo de identidade/ *identity theft*") e o uso desses dados (fraude de identidade/ *identity fraud*). Interessa ao presente trabalho a "usurpação da identidade" realizada com o fim de apropriação. Isto é: o usurpador precisa aparentar, perante terceiros, ser o legítimo titular dos dados. Quando essa aparência é estabelecida a conduta passa a nos interessar – e a avaliação deve ser feita caso a caso com base nesse critério.

3. USURPAÇÃO DA IDENTIDADE COMO MECANISMO VIABILIZADOR DA FRAUDE

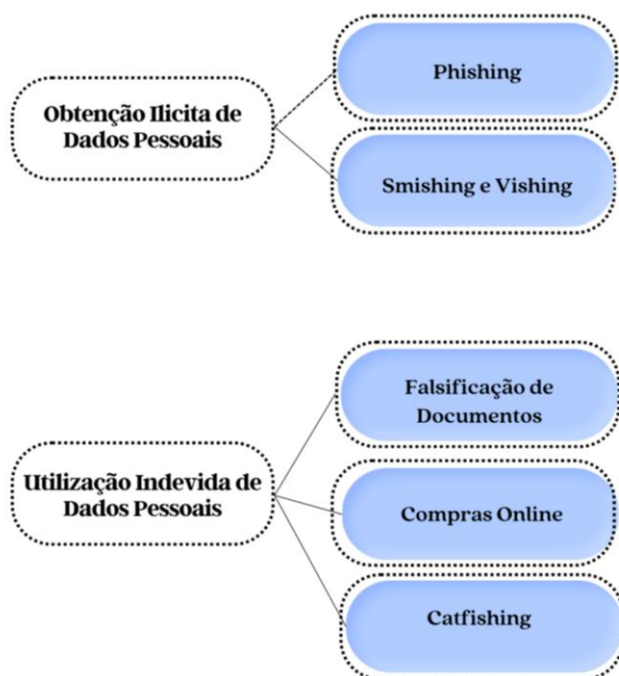
Como antecipado, o cenário em análise envolve o comportamento de terceiro que faz uso da identidade virtual de outra pessoa, assumindo a identidade dela, interagindo com seu círculo social, enviando mensagens, criando/utilizando um perfil e tirando proveito da confiança e preferências associadas a essa identidade. Isso resulta em uma apropriação completa da vida/identidade virtual dessa pessoa (e em certa medida "real"), englobando todos os seus aspectos e conquistas, os quais são alcançados à custa do esforço que ela dedicou para construí-los.⁶³

⁶³ Enquanto que a identidade legal é atribuída no momento do nascimento, com a atribuição de nome, números de identidade, sexo, local de nascimento, etc, a identidade virtual soma a legal com outro segmento maleável e construído de acordo com o interesse de cada usuário.

A conduta ilegal reside no uso indevido da confidencialidade e da credibilidade de outra pessoa em benefício próprio, seja por uso pessoal ou venda, sem o consentimento do titular dessas informações, resultando em prejuízos financeiros e emocionais adicionais. É necessário que a utilização da identidade virtual de outra pessoa seja realizada sem a devida autorização.⁶⁴

Como se intui, diversas ações criminosas podem, potencialmente, conduzir à apropriação indevida da identidade de alguém. Examinar-se-á, no próximo tópico, de que modo os dados podem ser obtidos. Posteriormente, analisar-se-á de que maneira os dados podem ser utilizados e os respectivos contextos legais aplicáveis. Observe-se esquemática e resumidamente:

Figura 5: Cibercrimes no contexto de Obtenção x Utilização Indevida de Dados Pessoais



Fonte: elaboração própria.

3.1. O PHISHING COMO MECANISMOS DE USO INDEVIDO DA IDENTIDADE ALHEIA

Em resumo, o *phishing* é um recurso de engenharia social. Trata-se de processo informático complexo que envolve a obtenção de informações pessoais de terceiros por meio do uso de e-mails falsos que direcionam o usuário para um link fraudulento. Nos links falsos, o

⁶⁴ BITTENCOURT, Cezar Roberto. **Tratado de Direito Penal** – Volume 3, 3ª Edição. São Paulo: Editora Saraiva, 2006. p. 15

usuário é levado a fornecer seus dados pessoais, acreditando erroneamente que está lidando com um interlocutor legítimo, como o seu banco pessoal ou um e-commerce, plataformas ou prestador de serviço para o qual normalmente forneceria essas informações – inclusive credenciais de acesso, como login e senha.⁶⁵

Figura 6: O ciclo da engenharia social



Fonte: Manage Engine. Reprodução de Guia sobre engenharia Social⁶⁶

Como se extrai da ilustração acima, os golpistas por trás do *phishing* geralmente criam e-mails, mensagens de texto, sites e outras formas de comunicação, disfarçadas de comunicações com aparência de genuinidade que estão vinculadas a empresas, instituições financeiras ou órgãos governamentais. Essa aparência de autenticidade, atribuída à sofisticação dos criminosos, torna difícil para os destinatários distinguir entre o legítimo e o fraudulento. Uma vez que os usuários caem na armadilha e fornecem suas informações, os criminosos podem usá-las para atividades ilegais, como apropriação indevida de identidade, fraude financeira e ataques subsequentes.

⁶⁵ REIS, Eva da Silva Rodrigues Pinto dos. **Apropriação Indevida de identidade:** enquadramento jurídico-penal. Dissertação de Mestrado – Universidade de Lisboa: Faculdade de Direito, 2019. p.20.

⁶⁶ Disponível em: <https://blogs.manageengine.com/portugues/2023/04/06/guia-sobre-engenharia-social-tudo-o-que-voce-precisa-saber.html>. Acesso em 21 nov 2023.

O envio de e-mails genéricos, sem segmentação, permite ao criminoso atingir uma grande quantidade de usuários com apenas o clique de um botão. Embora o conhecimento sobre esses ataques e as medidas preventivas tenham aumentado ao longo do tempo, ainda há muitas pessoas que não conseguem identificá-los – e a sofisticação dos criminosos cresce na mesma proporção das medidas de mitigação.⁶⁷

O uso de ferramentas como *cookies*, por exemplo, possibilita que os cibercriminosos adaptem o ataque a usuários específicos a partir do conhecimento de suas preferências e interesses (via "*spoofing*" e "*pharming*").

O *spoofing* é uma técnica que mascara o remetente de um e-mail, tornando-o parecido com o de outra pessoa, conferindo assim credibilidade à atividade fraudulenta, sem a necessidade de invadir a conta de e-mail de terceiros. No *pharming*, o e-mail não tem como objetivo obter dados sensíveis do destinatário, mas sim introduzir *malware* no computador do destinatário.

Nesse cenário, alguém pode receber um e-mail de uma instituição confiável, alertando sobre possíveis comprometimentos de sua conta ou dados e fornecendo orientações sobre como evitar isso. Geralmente, esses e-mails vêm com um link que faz o download de *malware*, ou seja, um *software* projetado para infiltrar-se ilegalmente no computador do usuário e obter seus dados. Uma vez que esses arquivos estão instalados, todas as atividades do usuário no computador são monitoradas.⁶⁸

3.2. O TITULAR COMO RESPONSÁVEL PELA APROPRIAÇÃO DE SUA IDENTIDADE POR TERCEIROS: SMISHING E VISHING

O termo "*smishing*" é uma combinação das palavras "SMS" (Short Message Service) e "*phishing*". Trata-se de uma técnica de engenharia social utilizada por cibercriminosos para tentar enganar pessoas por meio de mensagens de texto (SMS) em dispositivos móveis, como *smartphones*. O objetivo do *smishing* é persuadir a vítima a fornecer informações pessoais, financeiras ou confidenciais, clicar em links maliciosos ou baixar arquivos mal-intencionados.

⁶⁷ REIS, Eva da Silva Rodrigues Pinto dos. **Apropriação Indevida de identidade**: enquadramento jurídico-penal. Dissertação de Mestrado – Universidade de Lisboa: Faculdade de Direito, 2019. p.20.

⁶⁸ REIS, Eva da Silva Rodrigues Pinto dos. **Apropriação Indevida de identidade**: enquadramento jurídico-penal. Dissertação de Mestrado – Universidade de Lisboa: Faculdade de Direito, 2019. p.21.

Assim como o *phishing* (por e-mail), as mensagens de *smishing* geralmente são projetadas para parecerem legítimas, muitas vezes fingindo ser de uma empresa ou instituição confiável, como um banco, empresa de telecomunicações, agência governamental ou até mesmo serviços de entrega. Os criminosos enviam mensagens falsas com o intuito de induzir a vítima a tomar ações prejudiciais, como fornecer informações de cartão de crédito, senhas ou baixar aplicativos maliciosos que podem roubar dados do dispositivo.

No "*vishing*", a vítima fornece diretamente suas informações pessoais ao cibercriminoso, tipicamente por meio de uma chamada telefônica, seja realizada pelo criminoso ou por um sistema automático de chamadas que ele tenha criado. Nesse cenário, o cibercriminoso pode se fazer passar por alguém conhecido pela vítima, como mascarar o número de telefone para parecer ser de uma pessoa que a vítima reconheça, ou até mesmo representar uma instituição com a qual a vítima tenha relação, como um banco ou uma operadora de telefonia. O pretexto geralmente usado é a urgência de obter informações importantes, o que leva a vítima a divulgar seus dados pessoais. É relevante destacar que o "*vishing*" e o "*smishing*" frequentemente são utilizados em conjunto pelos criminosos para aumentar a credibilidade do golpe.⁶⁹

3.3. A RELAÇÃO ENTRE FALSIFICAÇÃO DE DOCUMENTOS E A USURPAÇÃO DA IDENTIDADE DIGITAL

É natural que, após a obtenção de dados pessoais alheios, os criminosos os utilizem, o que pode acontecer de várias formas. A falsificação de documentos é uma das mais costumeiras e pode incluir a criação de um documento de identificação completamente novo ou a adulteração de documentos oficiais, hipótese na qual se torna mais difícil identificar a fraude.

Os danos infligidos às vítimas podem variar substancialmente dependendo de como os dados são utilizados. Em muitos casos, os danos se traduzem principalmente em perdas financeiras diretas. Estas, a seu turno, podem ter repercussões duradouras, afetando a capacidade da vítima de obter crédito ou realizar compras – sendo comum que a vítima descubra a fraude no momento em que tenta, ela mesma sem sucesso, realizar transações financeiras válidas.

⁶⁹ REIS, Eva da Silva Rodrigues Pinto dos. **Apropriação Indevida de identidade**: enquadramento jurídico-penal. Dissertação de Mestrado – Universidade de Lisboa: Faculdade de Direito, 2019. p.22.

Além das perdas monetárias, as consequências podem se estender à reputação da vítima. Isso pode ocorrer de várias maneiras, inclusive mediante a criação de um registro criminal ilegítimo em nome da vítima. Da mesma forma, se os dados forem empregados para obter emprego, isso pode manchar a reputação profissional da vítima, potencialmente resultando em demissões ou dificuldades na busca de oportunidades de trabalho futuras.

3.4. IDENTIDADES DIGITAIS FALSAS E O CATFISHING

O *catfishing* é uma forma contemporânea do *phishing* que se baseia na criação de um perfil falso nas redes sociais com o objetivo de enganar outras pessoas, adotando uma identidade fictícia. Esse método pode ser utilizado tanto para obter quanto para usar dados. Quando um perfil online é construído usando informações pessoais de terceiros com a intenção de coletar informações de mais pessoas, estamos lidando com um caso de obtenção e uso de dados. No entanto, na maioria das vezes, o *catfishing* representa uma forma de uso de dados, não de obtenção. O objetivo principal de um *catfisher* é representar outra pessoa, escondendo sua identidade real. Para fazer isso, eles usam fotografias ou informações de indivíduos que consideram mais atraentes ou socialmente "populares". Mesmo quando não há uso de dados reais de terceiros, a finalidade subjacente é sempre a de enganar alguém, muitas vezes levando a vítima a compartilhar detalhes de sua vida íntima.

O desfecho legal dependerá das circunstâncias específicas do *catfishing*, como a utilização de fotografias, vídeos, conversas online ou a divulgação de detalhes da vida íntima da vítima⁷⁰. Além disso, as ações subsequentes do *catfisher*, como manter essas informações, divulgá-las ou usá-las para se aproximar da vítima, também influenciarão o enquadramento legal adequado para o caso.⁷¹

⁷⁰ A título exemplificativo: No ano de 2021, o caso do jogador italiano Roberto Cazzaniga, que acreditou namorar a modelo Alessandra Ambrósio por 15 anos, ganhou destaque nas redes sociais. No caso, o atleta foi enganado por uma mulher que usava as fotos da modelo para conseguir aplicar golpes. Disponível em: <https://www.tecmundo.com.br/internet/230164-caso-alessandra-ambrosio-catfish-protoger.htm>. Acesso em: 12 nov. 23.

Na mesma linha: Aposentada perde R\$ 208 mil achando que namorava Johnny Depp. Disponível em: <https://noticias.uol.com.br/colunas/rogerio-gentile/2022/10/04/aposentada-perde-r-208-mil-achando-que-namorava-johnny-depp.htm>. Acesso em: 12 nov. 23.

Espanhola investe quase um milhão de reais por acreditar estar em um relacionamento virtual com o ator Brad Pitt. Disponível em: <https://oglobo.globo.com/mundo/epoca/noticia/2023/06/brad-pitt-fake-mulher-perde-quase-um-milhao-de-reais-em-relacionamento-virtual.ghtml>. Acesso em: 12 nov. 23.

⁷¹ REIS, Eva da Silva Rodrigues Pinto dos. **Apropriação Indevida de identidade**: enquadramento jurídico-penal. Dissertação de Mestrado – Universidade de Lisboa: Faculdade de Direito, 2019. p.29.

3.5. A IDENTIDADE DIGITAL COMO ELEMENTO ESSENCIAL DA PERSONALIDADE DO INDIVÍDUO NA SOCIEDADE DE DADOS E A SUA FRAGILIDADE: O QUE É PRECISO PENSAR EM TERMOS DE CONSTRUÇÃO DE UMA TUTELA EFICAZ E QUE PAPEL O TITULAR EXERCE NESTE CENÁRIO?

Diante do que fora abordado, notório que a sociedade de dados, impulsionada pela constante evolução tecnológica, oferece inúmeras vantagens, mas também traz consigo ameaças significativas à identidade digital. A coleta massiva de dados, a proliferação de ciberataques e a comercialização desenfreada de informações pessoais representam sérios riscos para a privacidade e a segurança digital. A fragilidade da identidade digital é evidenciada por casos frequentes de violações de dados e usurpação de identidade, destacando a necessidade urgente de se repensar como são aplicadas as atuais medidas preventivas.

A análise da tutela da ciberidentidade, contudo, não pode se olvidar de que o titular da identidade digital desempenha um papel central e ativo na preservação da sua privacidade e na mitigação de riscos associados à crescente digitalização da sociedade.

A gestão proativa da presença online é uma pedra angular do empoderamento do titular. Isso implica não apenas criar uma presença digital, mas também monitorar e controlar ativamente as informações compartilhadas. A detecção precoce de sinais de acesso não autorizado ou comportamento anormal pode ser crucial para evitar potenciais violações de segurança. Isso envolve a análise regular das atividades em contas online, verificando registros de login e monitorando alertas de segurança. Ao ser proativo nesse aspecto, o titular pode identificar precocemente tentativas de comprometimento da sua identidade digital.

Portanto, o empoderamento do titular não se limita apenas à gestão técnica da identidade digital. Envolve também a consciência e a compreensão da importância das informações pessoais. O titular deve estar ciente dos riscos associados à divulgação indiscriminada de dados e compreender as implicações de suas escolhas online. Isso não apenas contribui para a própria segurança, mas também para a criação de uma cultura digital mais segura e consciente.

4. A TUTELA CONSTITUCIONAL-CIVIL DA CIBERIDENTIDADE E A RESPONSABILIDADE DO PRÓPRIO TITULAR

Após a definição do problema de pesquisa e da hipótese a ser examinada, este capítulo tem como finalidade apresentar os embasamentos teóricos do estudo, começando pela contextualização do tema no âmbito do Direito Constitucional.

A pesquisa, portanto, seguirá uma abordagem que integra as esferas do Direito Civil e Constitucional, incorporando as análises de autores que examinaram o processo de constitucionalização do Direito Civil. Nossa ênfase estará principalmente na área da responsabilidade civil, enfatizando a consagração dos princípios da solidariedade social e da dignidade da pessoa humana, além de promover a efetiva proteção das vítimas de danos.

Nessa abordagem, examinar-se-ão os elementos que caracterizam o dever de indenizar, a fim de avaliar se o conceito de responsabilidade civil é apropriado como uma solução legal para lidar com os danos decorrentes do uso não autorizado da identidade digital pessoal. Isso será feito levando em consideração os desafios e obstáculos que a doutrina tem destacado nesse contexto.

Para além dos pressupostos da responsabilidade civil, realizar-se-á a análise da participação do lesado na avaliação da conduta ilícita, isto sob a ótica da vitimologia.

Se compreenderá que a vitimologia desempenha um papel importante na análise da responsabilidade civil, especialmente quando se trata de determinar as implicações e consequências dos danos causados às vítimas porquanto a análise vitimológica busca compreender como as vítimas são afetadas pelos danos, tanto em termos físicos como emocionais, financeiros e sociais.

4.1. DIÁLOGO ENTRE A PROTEÇÃO DE IDENTIDADE DIGITAL E A RESPONSABILIDADE CIVIL: PANORAMA HISTÓRICO-TEÓRICO

Estabelecendo-se um paralelo com a proposta de reparação de danos advindos do uso da inteligência artificial no Brasil, autores como Tepedino e Silva⁷² argumentam que é essencial

⁷² TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. *Inteligência Artificial e Elementos da Responsabilidade Civil*. In: FRAZÃO, Ana.; MULHOLLAND, Caitlin. (Coord.). **Inteligência Artificial e Direito: Ética, Regulação e Responsabilidade**. 2. ed. São Paulo: Revista dos Tribunais, 2020. 29 p.

tratar essa questão de forma sistemática, levando em consideração a unidade e complexidade do ordenamento jurídico brasileiro.

Um dos pontos-chave levantados por esses autores é a necessidade de fundamentar a regulamentação da inteligência artificial na tábua axiológica constitucional. Isso implica considerar os valores e princípios consagrados na Constituição Brasileira, como a dignidade da pessoa humana, a privacidade, a igualdade e a justiça social. A partir dessa base constitucional, a responsabilidade civil e consumerista pode ser utilizada como um instrumento jurídico suficiente para lidar com questões relacionadas aos danos causados por sistemas autônomos.

Segundo os juristas, ao basear a regulamentação dos danos causados por sistemas autônomos nos princípios constitucionais que orientam a responsabilidade civil e o direito do consumidor, é possível resolver as questões decorrentes das novas tecnologias, enfatizando que as soluções legais para esses desafios não precisam ser necessariamente inéditas.⁷³

É importante reconhecer que estamos diante de desafios diferentes daqueles enfrentados durante as Revoluções Industriais. A coleta massiva de dados pessoais, o uso de reconhecimento facial, carros autônomos e outras tecnologias introduzem novas complexidades e riscos. Isso exige uma abordagem jurídica atualizada e adaptada às especificidades da Era Digital.

Além disso, é fundamental compreender a evolução da disciplina da responsabilidade civil ao longo do tempo. O direito privado passou por uma transformação significativa, afastando-se dos valores individualistas e patrimonialistas do passado para se alinhar com os postulados existenciais da Constituição. Isso implica que o direito deve considerar não apenas danos materiais, mas também danos morais e existenciais, refletindo a mudança de paradigma na sociedade.

Para entender o ponto em que nos encontramos atualmente, é relevante analisar a trajetória pela qual a área da responsabilidade civil evoluiu à medida que o campo do direito privado se distanciou dos princípios individualistas e patrimoniais para se alinhar com os princípios existenciais estabelecidos na Constituição.

A transformação da responsabilidade civil ao longo da história do Direito é uma narrativa que ilustra a adaptabilidade desse campo jurídico às mudanças sociais e culturais.

⁷³ TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. *Inteligência Artificial e Elementos da Responsabilidade Civil*. In: FRAZÃO, Ana.; MULHOLLAND, Caitlin. (Coord.). **Inteligência Artificial e Direito: Ética, Regulação e Responsabilidade**. 2. ed. São Paulo: Revista dos Tribunais, 2020. p. 307.

Inicialmente, a concepção de responsabilidade era impregnada de crenças antigas, em que a culpa era frequentemente atribuída aos deuses ou ao destino⁷⁴. Esse entendimento ancestral se afastou gradualmente com o desenvolvimento do Direito, e uma das etapas marcantes foi a proibição da autotutela, que encerrou a ideia de “olho por olho, dente por dente”, substituindo-a por um sistema mais organizado e justo de resolução de disputas.

No entanto, a verdadeira revolução na responsabilidade civil surgiu quando a culpa passou a ser vinculada diretamente à ocorrência de danos. Isso representou uma mudança fundamental, pois permitiu que as vítimas buscassem reparação não apenas com base na intenção do agente causador, mas também quando a negligência ou a imprudência estavam envolvidas. Essa evolução tornou possível responsabilizar aqueles que, de forma não intencional, causavam prejuízos a terceiros.

Nos tempos mais recentes, o conceito de responsabilidade civil ampliou-se ainda mais ao incorporar o princípio do risco. Isso significa que, mesmo na ausência de culpa direta, a pessoa ou entidade responsável pode ser obrigada a reparar os danos causados, especialmente em casos que envolvem atividades de alto risco. Além disso, essa abordagem engloba não apenas danos individuais, mas também danos coletivos, reconhecendo que certas ações podem prejudicar grupos inteiros da sociedade.

Essa evolução da responsabilidade civil permitiu que a lei fosse aplicada de maneira mais abrangente, abarcando não apenas danos patrimoniais, mas também danos de natureza extrapatrimonial, como danos morais e à dignidade da pessoa. Além disso, a possibilidade de cumular essas formas de reparação tornou o sistema mais flexível e adaptável a uma ampla gama de situações.

Atualmente, é indiscutível que a responsabilidade civil vai muito além de ser simplesmente um mecanismo para resolver disputas entre indivíduos, sem relevância ou impacto na sociedade ou no Estado⁷⁵. Isso ocorre porque o verdadeiro propósito do instituto, em sua essência, é a proteção da própria dignidade humana, ou seja, a responsabilidade civil

⁷⁴ Marco Fabio Morsello explica que desde os primórdios do *Homo sapiens*, prosseguindo-se na Antiguidade, os acontecimentos tinham aspecto fatalista, místico e religioso, de forma que o acaso era decorrente da “vontade incontornável dos Deuses”. Assim, foi o ‘desafio aos deuses’, expressão do livro de Peter L. Bernstein, pondo o “futuro a serviço do presente, compreendendo o risco, medindo-o e transformando-o em um dos principais catalizadores que impelem a sociedade moderna”. In: MORSELLO, Marco Fábio. **Contrato de Transporte: novos paradigmas do caso fortuito e força maior**. São Paulo: Thomson Reuters Brasil, 2021. p. 28 e 85.

⁷⁵ MATOS, Eneas de Oliveira. **Dano moral e dano estético**. Rio de Janeiro: Renovar, 2008. p. 2.

desloca seu foco do agente causador para a vítima do dano injusto, alterando-se os critérios da reparação.⁷⁶

Essa abordagem ampla da dignidade da pessoa humana como um princípio unificador tem impacto em diversos campos do Direito, incluindo o direito civil, o direito penal, o direito do trabalho, entre outros. Os tribunais e os legisladores são instados a considerar a dignidade como um valor fundamental em todas as suas decisões e ações.

Por outro lado, a transição de regimes ditatoriais para democracias ao redor do mundo trouxe consigo uma profunda reflexão sobre a necessidade de proteger a dignidade e os interesses da pessoa humana. Afinal, quem cria um risco deve responder por suas consequências.

Essa preocupação é ainda mais relevante na chamada quarta era de direitos, caracterizada por avanços tecnológicos exponenciais e pelo desenvolvimento de atividades cujos riscos muitas vezes são desconhecidos. Novas tecnologias, como inteligência artificial, biotecnologia e nanotecnologia, trazem consigo potenciais benefícios extraordinários, mas também carregam riscos complexos e incertos.

Ao lado das vantagens proporcionadas pelo progresso tecnológico, observa-se uma crescente carga de riscos de danos à pessoa⁷⁷, tanto em termos materiais quanto morais. Isso reforça a necessidade premente de atenção às questões de responsabilidade civil e à apreciação de novos institutos legais para garantir a adequação da reparação em caso de danos.

A doutrina jurídica enfatiza que o dever de indenizar é fundamentado na máxima "*honestae vivere, alterum non laedere, suum cuique tribuere*", que pode ser traduzida como "viver honestamente, não lesar a outrem e dar a cada um o que é seu". Essa máxima alberga os princípios fundamentais que regem a responsabilidade civil, e sua essência está contida nos princípios do *neminem laedere* (não lesar a ninguém) e do *alterum non laedere* (não lesar outrem).⁷⁸

Dentro desse contexto, o instituto da responsabilidade civil desempenha um papel crucial como um catalisador dos princípios da prevenção e da precaução. Isso significa que as

⁷⁶ PEREIRA, Caio Mário da Silva. **Responsabilidade civil**. 10. ed. Rio de Janeiro: GZ, 2012. p. 14.

⁷⁷ "(...) os bônus dos avanços tecnológicos representam o ônus de uma maior chance de incidentes e de maior gravidade e alcance das lesões." *In*: SOARES, Flaviana Rampazzo. **Responsabilidade civil por dano existencial**. [s.l.], 2009, p. 23.

⁷⁸ STOCO; Rui. **Tratado de responsabilidade civil: doutrina e jurisprudência**. São Paulo: Editora Revista Dos Tribunais, 2007. p. 114.

peessoas têm o dever de evitar causar danos injustos a terceiros, e caso ocorram tais danos, é responsabilidade delas tomar medidas para evitar que o dano se agrave ainda mais. Esse conceito é muitas vezes referido como "*duty to mitigate the loss*" (dever de mitigar a perda).⁷⁹

A objetivação da responsabilidade, ou seja, o dever de reparar independentemente da comprovação da culpa, surgiu de maneira progressiva ao longo do tempo, sendo estabelecida por meio de leis especiais⁸⁰.

No entanto, a verdadeira revolução na objetivação da responsabilidade ocorreu com a Constituição Federal de 1988. A Constituição consolidou a possibilidade de indenização por danos morais (artigo 5º, incisos V e X), estabeleceu a responsabilidade objetiva do Estado e de todos os prestadores de serviços públicos, como luz, gás, telefonia, transportes, etc. (§6º do artigo 37), disciplinou a responsabilidade por ato judicial (artigo 5º, inciso LXXV), por dano nuclear (artigo 21, inciso XXIII, letra c) e danos ao meio ambiente (artigo 225, § 3º).

No entanto, o golpe final à responsabilidade subjetiva ocorreu com a promulgação do Código de Defesa do Consumidor em 1990⁸¹. Esse código estabeleceu uma mudança de paradigma ao transferir os riscos do consumo para o fornecedor. Adotou-se o sistema da responsabilidade objetiva para todos os casos de acidente de consumo, independentemente de serem decorrentes do fato do produto (artigo 12) ou do fato do serviço (artigo 14). Isso significa que o consumidor passou a ter um nível mais elevado de proteção, não precisando mais provar a culpa do fornecedor em casos de danos causados por produtos ou serviços defeituosos.

No contexto da responsabilidade objetiva, o indivíduo que causou o dano só será liberado de sua obrigação de reparação se puder demonstrar a presença de circunstâncias que excluam a responsabilidade, seja porque interrompem a relação de causa e efeito ou porque eliminam a ilicitude de sua conduta.

A tendência predominante nos tempos atuais é a mutualização ou socialização dos riscos, refletindo uma mudança significativa na maneira como a sociedade lida com questões

⁷⁹ BRAGA NETTO, Felipe Peixoto; FARIAS, Cristiano Chaves; ROSENVALD, Nelson. **Novo Tratado de Responsabilidade Civil**. 3. ed. São Paulo: Saraiva Educação, 2018. p. 53-54.

⁸⁰ Um exemplo inicial dessa mudança foi observado em legislações específicas, como a Lei das Estradas de Ferro, Acidente do Trabalho, Seguro Obrigatório, Dano ao Meio Ambiente, entre outras. Essas leis começaram a reconhecer a necessidade de responsabilização independentemente da culpa e a estabelecer normas específicas para casos de danos.

⁸¹ CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. 15. ed. Barueri: Atlas, 2021. p. 30.

de responsabilidade civil⁸². A mutualização ou socialização dos riscos envolve a ideia de que, em muitos casos, é mais justo e eficiente que a sociedade como um todo assuma a responsabilidade por determinados riscos, em vez de atribuí-los unicamente ao indivíduo que causou o dano. Isso se alinha com a ideia de uma maior solidariedade social e uma abordagem mais equitativa para lidar com os danos causados pela atividade humana.

De toda sorte, os pressupostos da responsabilidade civil geralmente incluem a conduta ilícita, o dano, o nexo causal e a ausência de excludentes de responsabilidade. A análise sistemática das disposições presentes no Código Civil, no Código de Defesa do Consumidor, no Marco Civil da Internet e na LGPD desempenha um papel fundamental nesse contexto, uma vez que esses microssistemas podem fornecer orientações adicionais sobre as excludentes de responsabilidade e como elas se aplicam em diferentes contextos legais.

Portanto, em um contexto em que a mutualização e a socialização dos riscos ganham destaque, é crucial entender não apenas os deveres de indenização, mas também as circunstâncias em que a responsabilidade civil pode ser afastada. Isso promove uma abordagem mais equilibrada e justa para lidar com os danos causados em uma sociedade cada vez mais complexa e interconectada.

4.2. A PROTEÇÃO DA CIBERIDENTIDADE NO CONTEXTO DA SOCIEDADE DE DADOS: O DIREITO PRECISA ASSIMILAR A REALIDADE ALGORÍTMICA E SUAS CONSEQUÊNCIAS PRÁTICAS

Como se viu, no Código Civil de 1916, o instituto da responsabilidade civil seguia uma lógica que se baseava na prática de um ato ilícito, fundamentado em uma cláusula geral que, para estabelecer seu elemento essencial, exigia a comprovação da culpa⁸³. Ou seja, a responsabilidade civil era determinada pela presença de culpa por parte do agente que havia causado o dano. Para que a vítima pudesse buscar uma indenização, era necessário não apenas demonstrar o prejuízo sofrido, mas ainda provar que o agente agiu com culpa e estabelecer o nexo de causalidade entre a conduta do agente e o dano causado. Esses requisitos funcionavam

⁸² “O que predomina é a inclinação para a socialização dos riscos, e com ela a da responsabilidade civil. No seu entusiasmo e otimista, o Prof. Wilson Melo da Silva sustenta que ‘a socialização dos riscos, pois, oferece perspectivas promissoras. Não leva ao cerceamento da livre atividade e da iniciativa de ninguém, criando para a vítima possibilidade de uma indenização sempre garantida’. *In*: PEREIRA, Caio Mário da Silva. **Responsabilidade Civil**. Atualizador: Gustavo Tepedino. 12. ed. rev., atual. e ampl. – Rio de Janeiro: Forense, 2018. p. 14.

⁸³ MORAES, Maria Celina Bodin de. Risco, solidariedade e responsabilidade objetiva. **Revista dos Tribunais**, v. 854, 2006. p. 11-37.

como critérios rigorosos que filtravam as demandas de ressarcimento que chegavam ao Poder Judiciário.⁸⁴

Essa abordagem estava alinhada com a concepção liberal da época, que valorizava a autonomia privada e restringia a intervenção estatal apenas em casos de uso flagrantemente ilegítimo da liberdade individual. Com efeito, o sistema jurídico estava estruturado de forma a proteger a liberdade das partes envolvidas em um litígio, garantindo que somente em situações em que ficasse clara a culpa do agente e sua responsabilidade direta pelo dano é que uma demanda de indenização seria acolhida.

Esse modelo de responsabilidade civil – baseado na culpa e na necessidade de comprovação rigorosa dos elementos essenciais – tinha suas vantagens, pois promovia a segurança jurídica e evitava o excesso de litigância. No entanto, também tinha suas limitações, uma vez que, em alguns casos, tornava difícil para as vítimas obterem a devida compensação, especialmente quando a culpa do agente não era evidente.

A ideia de imputar a alguém a responsabilidade de indenizar sem necessariamente cometer um ato ilícito é uma característica da sociedade industrializada. Com o tempo, a evolução da sociedade e das relações jurídicas levou a mudanças significativas nesse paradigma da responsabilidade civil. Novos modelos legais surgiram, como a responsabilidade objetiva, que não exige a comprovação de culpa, e novos princípios orientaram a análise de casos de responsabilidade civil. Tais mudanças refletiram a necessidade de adaptar o sistema jurídico à complexidade das relações sociais e econômicas modernas, buscando um equilíbrio entre a proteção dos direitos individuais e a justa reparação dos danos sofridos pelas vítimas.

Neste mesmo sentido, é pertinente reconhecer a sociedade de risco como tal, conforme teorizado por Ulrich Beck em 1992. A função da responsabilidade civil se transforma substancialmente. Em vez de se concentrar principalmente na punição do agente causador do dano, o novo paradigma coloca a reparação dos danos sofridos pela vítima como prioridade. Isso ocorre porque, sob a lógica estrita da culpa, os danos considerados inevitáveis não corresponderiam a qualquer forma de reparação civil.⁸⁵

⁸⁴ SCHREIBER, Anderson. **Novos Paradigmas da Responsabilidade Civil**: da erosão dos filtros da reparação à diluição dos danos. São Paulo: Editora Atlas, 2ª ed., 2009. 276 p.

⁸⁵ MORAES, Maria Celina Bodin de. Risco, solidariedade e responsabilidade objetiva. **Revista dos Tribunais**, v. 854, 2006.

A superação da tradicional abordagem moralizadora e punitiva da responsabilidade civil abre espaço para uma compreensão mais ampla e contemporânea. Esse novo entendimento se baseia em um dever geral de solidariedade, que encontra respaldo no artigo 3º, inciso I, da Constituição de 1988. Esse dispositivo estabeleceu a obrigação de agir de forma a não prejudicar os interesses de terceiros, refletindo a evolução dos conceitos jurídicos para se adaptar às demandas de uma sociedade em constante transformação.⁸⁶

Portanto, diante dos desafios de uma sociedade de risco, a responsabilidade civil não se limita a sancionar o agente culpado, mas busca restabelecer o equilíbrio e proporcionar reparação às vítimas. Ela desempenha um papel fundamental na procura por soluções justas e equitativas em um mundo cada vez mais complexo e interconectado.

Nesse diapasão, a Constituição de 1988 marcou o início de um novo contexto axiológico no ordenamento jurídico brasileiro ao consagrar um compromisso claro com a proteção da vítima de danos. Essa mudança de perspectiva constitucional teve repercussões significativas no nível infraconstitucional, como evidenciado pela promulgação do Código de Defesa do Consumidor, que instituiu a responsabilidade objetiva do fornecedor de produtos e serviços, como destacado por Schreiber (2009). O Código Civil de 2002 seguiu a mesma tendência ao estabelecer a responsabilidade objetiva em situações em que o código anterior presumia a culpa. Isso se aplica, por exemplo, à responsabilidade por atos de terceiros e por atos de animais⁸⁷.

Com a mudança de paradigma, o foco da preocupação não está mais exclusivamente no sujeito responsável pelo dano, mas sim na reparação do prejuízo sofrido pela vítima. Além disso, a esfera patrimonial individual cede espaço para a proteção de situações existenciais que dizem respeito à sociedade como um todo. Isso reflete uma lógica de justiça distributiva, que visa não apenas punir o responsável pelo dano, mas também garantir que as vítimas sejam adequadamente compensadas.⁸⁸

O que se tornou evidente foi que a disciplina da responsabilidade civil contemporânea, ancorada em uma perspectiva constitucionalizada e guiada pela unidade e completude do

⁸⁶ MORAES, Maria Celina Bodin de. Risco, solidariedade e responsabilidade objetiva. **Revista dos Tribunais**, v. 854, 2006.

⁸⁷ SCHREIBER, Anderson. **Novos Paradigmas da Responsabilidade Civil**: da erosão dos filtros da reparação à diluição dos danos. São Paulo: Editora Atlas, 2ª ed., 2009.

⁸⁸ EHRHARDT JÚNIOR, Marcos. Responsabilidade Civil ou Direito de Danos? Breves reflexões sobre a inadequação do modelo tradicional sob o prisma do Direito Civil Constitucional. *In*: RUZYK, Carlos Eduardo Pianosvki et al. (Org.). **Direito Civil Constitucional**: a ressignificação da função dos institutos fundamentais do direito civil contemporâneo e suas consequências. Florianópolis: Conceito, 2014. p. 19-27.

ordenamento jurídico, oferece um arcabouço teórico adequado para abordar os danos mencionados anteriormente.

4.3. A TUTELA DA VÍTIMA DE DANOS: UMA ANÁLISE A PARTIR DOS PRESSUPOSTOS DA RESPONSABILIDADE CIVIL

4.3.1. Ato ilícito

O ato ilícito, no contexto do direito civil, é uma conduta que pode ser classificada como contrária ao ordenamento jurídico e que viola direitos, caracterizando assim a antijuridicidade. Isso pode ocorrer tanto por meio de uma ação ativa quanto por omissão do agente, desde que essa conduta seja voluntária e consciente, o que envolve o elemento subjetivo da imputabilidade.

A antijuridicidade, como elemento objetivo do ato ilícito, consiste na transgressão aos deveres jurídicos e na ofensa a direitos legalmente protegidos. Quando alguém pratica uma ação que vai contra as normas legais ou deixa de cumprir uma obrigação legal, está agindo de forma antijurídica. Isso significa que a sua conduta é considerada ilegal e passível de sanções.

Por outro lado, a imputabilidade, como elemento subjetivo, refere-se à capacidade do agente para responder pelos seus atos. Em geral, presume-se que uma pessoa é capaz para os atos da vida civil a partir dos 18 anos, conforme estabelecido no artigo 5º do Código Civil. No entanto, existem exceções, como quando uma pessoa é declarada incapaz nos termos dos artigos 3º e 4º do Código Civil, ou quando há causas de incapacidade específicas previstas no artigo 928 do Código Civil e no artigo 116 do Estatuto da Criança e do Adolescente.

Além disso, a imputabilidade leva em consideração se o agente voluntariamente se coloca em estado de inimputabilidade transitória, como no caso da embriaguez, que pode reduzir a capacidade de discernimento do agente. Por fim, a imputabilidade verifica se o agente não está sujeito a uma interdição legal, conforme estabelecido no artigo 1.767 do Código Civil.

Em resumo, o ato ilícito envolve a antijuridicidade, que é a violação de deveres jurídicos e a ofensa a direitos, juntamente com a imputabilidade, que avalia a capacidade do agente para responder pelos seus atos. Ambos os elementos são fundamentais na análise e na caracterização do ato ilícito no contexto do direito civil.

No caso de usurpação de identidade, a ilicitude da conduta está intrinsecamente ligada ao uso indevido da confidencialidade e da credibilidade alheias em benefício próprio, seja através do uso ou venda da identidade virtual usurpada, sem o consentimento do titular legítimo. Além disso, essa prática muitas vezes resulta em danos patrimoniais e emocionais significativos para a vítima.

A essência deste ilícito reside no fato de que alguém se apropria de informações pessoais de outra pessoa, como nome, imagem, perfil em redes sociais, ou outros dados de identificação, e utiliza essas informações de maneira fraudulenta, muitas vezes com o intuito de cometer fraudes financeiras, difamação, ou outros atos prejudiciais. É fundamental notar que, para que a conduta seja considerada ilícita, o uso da personalidade virtual alheia deve ocorrer sem a devida autorização do titular legítimo.

No entanto, é importante destacar que a permissão concedida pelo titular da identidade virtual pode mudar o contexto legal da situação. Por exemplo, se alguém autoriza outra pessoa a enviar mensagens em seu nome ou a usar seu apelido em uma conversa, isso não constitui uma violação de um bem jurídico, uma vez que o consentimento do titular exclui o caráter furtivo da ação. O consentimento da vítima é fundamental, e sua ausência é o que torna a conduta de usurpação de identidade ilícita.

Portanto, a análise da ilicitude da usurpação de identidade envolve a verificação de se houve autorização prévia do titular legítimo para o uso da identidade virtual. A falta de consentimento da vítima é um elemento crucial para estabelecer a antijuridicidade da conduta, uma vez que, na presença de autorização, a ação pode não configurar uma violação dos direitos do titular legítimo.

4.3.2. O nexa causal: Prova de prejuízos e dificuldades na reparação

A crescente integração das tecnologias digitais emergentes em nossa sociedade trouxe consigo uma série de desafios significativos para o campo da responsabilidade civil. Monteiro Filho e Rosenvald (2020) identificam vários atributos dessas tecnologias que complicam a atribuição de responsabilidade por danos decorrentes de seu uso. Vamos analisar esses atributos com mais detalhes:

Tabela 1: Atributos das tecnologias digitais e suas implicações no campo da responsabilidade Civil

Complexidade:	As tecnologias digitais emergentes frequentemente envolvem uma rede complexa de atores em seu desenvolvimento, desde designers de hardware até programadores de software e fornecedores de serviços. Essa complexidade torna difícil determinar quem é responsável por um eventual dano, pois muitos indivíduos ou entidades podem ter contribuído de alguma forma.
Opacidade:	A natureza opaca das tecnologias digitais significa que os processos que ocorrem dentro delas podem ser difíceis de entender e rastrear. Isso torna desafiador identificar com precisão o que causou um dano específico e quem deve ser responsabilizado por ele.
Abertura:	Muitas tecnologias digitais são projetadas para serem atualizadas continuamente, muitas vezes após já estarem em uso. Isso significa que podem ocorrer mudanças significativas em seu funcionamento ao longo do tempo, o que complica a avaliação de quem é responsável por problemas que surgem após uma atualização.
Autonomia:	As tecnologias digitais emergentes frequentemente têm a capacidade de operar de forma autônoma, executando tarefas sem a necessidade de supervisão humana constante. Isso levanta a questão de quem é responsável quando uma máquina autônoma causa danos, uma vez que não há uma pessoa diretamente envolvida no momento do incidente.
Vulnerabilidade:	A crescente conectividade das tecnologias digitais também as torna mais suscetíveis a violações de segurança cibernética. Quando ocorrem violações, pode ser difícil determinar quem é responsável pelos danos resultantes e como eles poderiam ter sido evitados.
Imprevisibilidade:	Muitas dessas tecnologias são programadas para responder a estímulos variados e podem tomar decisões com base em algoritmos complexos. Isso cria um grau de imprevisibilidade, uma vez que podem reagir a situações não previstas pelos desenvolvedores, o que complica a avaliação de responsabilidade em caso de danos.

Todas essas características apontadas por Monteiro Filho e Rosenvald tornam a atribuição de responsabilidade por danos facilitados por tecnologias digitais emergentes uma tarefa complexa. A determinação do liame causal entre uma pessoa envolvida na utilização indevida da tecnologia e o dano resultante pode ser desafiadora devido à natureza multifacetada

e evolutiva dessas tecnologias. Como resultado, a legislação e a jurisprudência estão constantemente enfrentando o desafio de adaptar as normas de responsabilidade civil para lidar com esses novos cenários, buscando um equilíbrio entre a inovação tecnológica e a proteção dos direitos individuais e coletivos.

A aferição do nexo causal desempenha um papel fundamental no sistema de responsabilidade civil, pois estabelece a conexão entre a conduta do agente e o dano causado à vítima. No entanto, ao longo do tempo, essa avaliação do nexo causal passou por mudanças significativas, especialmente à medida que o conceito de culpa perdeu parte de sua importância no sistema de responsabilidade civil. O arrefecimento da culpa permitiu uma abordagem mais flexível e adaptável à reparação dos danos, superando a ideia de que o nexo causal deve ser uma barreira intransponível.

Autores como Schreiber⁸⁹ e Ramos⁹⁰ observam que o Poder Judiciário tem atribuído certa elasticidade ao requisito do nexo causal, com o objetivo de assegurar maior reparação às vítimas de danos. Isso significa que os tribunais estão dispostos a considerar uma variedade de fatores na análise do nexo causal, em vez de aplicar uma abordagem estritamente rígida.

A complexidade dessa questão é agravada pela multiplicidade de teorias que buscam explicar as relações de causalidade. Essas teorias podem variar ligeiramente entre si, o que leva a um "ecletismo judicial" em que os tribunais têm liberdade para escolher a teoria que melhor se adequa ao caso concreto. Essa preferência pela "justiça" no caso específico, em detrimento da previsibilidade dos resultados, pode levar a decisões judiciais divergentes.⁹¹

A falta de um consenso doutrinário significativo em torno da matéria também contribui para a aplicação de teorias diversas pelos tribunais. Isso significa que não existe um padrão claro nas decisões judiciais que deferem pedidos de reparação por danos, o que pode tornar a jurisprudência menos previsível.⁹²

⁸⁹ SCHREIBER, Anderson. **Novos Paradigmas da Responsabilidade Civil**: da erosão dos filtros da reparação à diluição dos danos. São Paulo: Editora Atlas, 2ª ed., 2009.

⁹⁰ RAMOS, André Luiz Arnt. A responsabilidade civil para além dos esquemas tradicionais: prospecções do dano reparável na contemporaneidade. **Revista Fórum de Direito Civil - RFDC**. Belo Horizonte, ano 4, n. 10, p. 13-33, set./dez., 2015.

⁹¹ COUTINHO, Marina de Alencar Araripe. **A proteção da vítima de danos causados por uma inteligência artificial**: uma perspectiva civil-constitucional. Orientador: Prof. Dr. Fabiano Hartmann. 2022. 129 p. Dissertação (Mestrado no curso de Direito) - Universidade de Brasília, Brasília, 2022. p.69.

⁹² SCHREIBER, Anderson. **Novos Paradigmas da Responsabilidade Civil**: da erosão dos filtros da reparação à diluição dos danos. São Paulo: Editora Atlas, 2ª ed., 2009.

Entre as teorias existentes, Schreiber (2009) e Tepedino (2017) destacam quatro abordagens principais para entender o nexa causal:

Tabela 2: Teorias de análise do nexa causal na Responsabilização Civil

<p>Teoria da Equivalência das Condições</p>	<p>Esta teoria estabelece que qualquer evento que tenha contribuído de alguma forma para a produção do dano deve ser considerado como causa para fins de responsabilização. Em outras palavras, todos os eventos que concorreram, de alguma maneira, para o resultado danoso são tratados como causas igualmente válidas. Essa teoria adota um critério de causalidade ampla, abrangendo todas as condições que contribuíram, mesmo que de forma mínima, para o dano.</p>
<p>Teoria da Causalidade Adequada</p>	<p>A teoria da causalidade adequada busca identificar, entre as possíveis causas, qual delas, em abstrato, é a mais apta a produzir o efeito danoso. Em outras palavras, procura-se determinar qual causa é a mais relevante ou adequada para a ocorrência do dano, com base em critérios de probabilidade ou plausibilidade. Essa abordagem se concentra em identificar a causa que, teoricamente, teria maior potencial para causar o dano.</p>
<p>Teoria da Causalidade Eficiente</p>	<p>A teoria da causalidade eficiente busca eleger, no caso concreto, o antecedente que, devido a um poder qualitativo ou quantitativo, pode ser considerado como causa do evento. Ela considera não apenas a contribuição de eventos para o dano, mas também a eficiência ou importância de cada um deles na produção do resultado danoso. Essa abordagem enfatiza a análise das características específicas do evento em questão.</p>
<p>Teoria da Causa Direta e Imediata (Subteoria da Necessariedade Causal)</p>	<p>De acordo com esta teoria, apenas os eventos que estão vinculados diretamente e imediatamente ao prejuízo podem ser considerados como causas. Eventos indiretos e remotos são excluídos, a menos que sejam consequência necessária da conduta tomada como causa. Essa abordagem estabelece um critério mais estrito para a causalidade, requerendo uma conexão direta e imediata entre a ação e o dano.</p>

A escolha da teoria a ser aplicada pode variar de acordo com a jurisdição, o contexto do caso e as normas legais vigentes. A falta de um consenso doutrinário significativo em torno da matéria, como mencionado anteriormente, pode levar os tribunais a aplicar teorias diversas, dependendo das circunstâncias específicas de cada caso. Essa variedade de abordagens pode

tornar a determinação do nexu causal um desafio complexo na prática jurídica, com implicações importantes para a responsabilização e a reparação de danos.

Por outro lado, tem sido observado um rigor crescente na interpretação e no reconhecimento das excludentes de causalidade, especialmente no que diz respeito a quatro delas: caso fortuito, força maior, culpa exclusiva da vítima e fato de terceiro.

Tabela 3: Excludentes de Causalidade - Caso Fortuito, Força Maior, Culpa exclusiva da Vítima e Fato de Terceiro

Caso Fortuito e Força Maior	Tradicionalmente, o caso fortuito e a força maior são eventos imprevisíveis e inevitáveis que podem interromper o nexu causal, isentando o agente de responsabilidade. No entanto, tem havido uma evolução na interpretação dessas excludentes. A noção de "fortuito interno", desenvolvida no contexto das relações consumeristas, amplia a responsabilidade do fornecedor. Ela implica que, mesmo que um evento seja imprevisível e inevitável, o fornecedor pode ser responsabilizado se esse evento pudesse ter sido detectado antes da disponibilização do produto no mercado. Isso reflete uma preocupação maior com a proteção do consumidor e a ideia de que os fornecedores devem assumir uma parcela do risco inerente à comercialização de produtos. ⁹³
Culpa Exclusiva da Vítima:	A culpa exclusiva da vítima tradicionalmente interrompe o nexu causal, isentando o responsável pelo dano de responsabilidade. No entanto, o Poder Judiciário tem interpretado essa excludente de forma restritiva em certos casos. Isso significa que, mesmo que a vítima tenha agido de forma negligente ou imprudente, sua culpa não necessariamente exclui a responsabilidade do agente causador do dano. ⁹⁴
Fato de Terceiro:	De maneira semelhante, o fato de terceiro, que se refere a ações de terceiros que interrompem o nexu causal, também tem sido interpretado de forma restritiva pelo Poder Judiciário. Em muitas situações, ações de terceiros que contribuem para um dano não excluem a responsabilidade do agente causador do dano. Novamente, essa interpretação restritiva deveria buscar garantir que o agente responsável assumisse uma parcela

⁹³ SCHREIBER, Anderson. **Novos Paradigmas da Responsabilidade Civil:** da erosão dos filtros da reparação à diluição dos danos. São Paulo: Editora Atlas, 2ª ed., 2009.

⁹⁴ SCHREIBER, Anderson. **Novos Paradigmas da Responsabilidade Civil:** da erosão dos filtros da reparação à diluição dos danos. São Paulo: Editora Atlas, 2ª ed., 2009.

	do risco associado à sua atividade, especialmente quando essa atividade envolve potenciais danos a terceiros. ⁹⁵
--	---

A questão da dificuldade em estabelecer uma conexão precisa entre um dano sofrido e a ação ou omissão de um agente específico tem levado a uma série de discussões no campo da responsabilidade civil. Isso se reflete na mitigação da prova da culpa, onde a investigação da causalidade muitas vezes pode resultar em múltiplas respostas ou mesmo na ausência de uma resposta clara. Essa complexidade na determinação do nexo causal levanta preocupações e desafios significativos.

Uma das razões por trás da mitigação da prova da culpa é a preocupação com a proteção das vítimas de danos. Quando uma vítima não consegue demonstrar com precisão a conexão entre o dano e a conduta de um agente específico, pode enfrentar dificuldades em buscar reparação. No entanto, como aponta Schreiber (2009), é importante exercer cautela ao lidar com essa questão. A liberalização excessiva das regras de causalidade pode potencialmente levar à multiplicação de demandas por indenização e à criação de uma cultura de vitimização social⁹⁶, em que as pessoas buscam responsabilizar terceiros por eventos indesejados de forma indiscriminada.

Ao tratar desta questão, Mulholland⁹⁷ propõe uma fundamentação jurídica adequada para a aferição do nexo de causalidade, considerando a sistematização das hipóteses em que o uso da presunção como meio de prova é justificável no âmbito da responsabilidade civil. Ela argumenta que o nexo de causalidade não deve ser visto apenas como um elemento de fato, mas deve incluir um elemento jurídico na investigação.

A autora sugere que a teoria da causalidade adequada pode ser a abordagem mais adequada para a aferição probabilística do evento danoso. Essa teoria considera a aptidão para

⁹⁵SCHREIBER, Anderson. **Novos Paradigmas da Responsabilidade Civil**: da erosão dos filtros da reparação à diluição dos danos. São Paulo: Editora Atlas, 2ª ed., 2009.

⁹⁶ “Inspirada na solidariedade social, a jurisprudência tem, por toda parte, se recusado a deixar as vítimas dos danos sem reparação. As cortes flexibilizam, deste modo, a configuração dos pressupostos da responsabilização, no solidário reconhecimento de que, de alguma forma, por vivermos em sociedade, todos somos culpados por todos os danos e todos somos causadores de todos os danos. Este itinerário, todavia, se conclui, atualmente, com o lançamento do dever de indenizar sobre um único agente, despertando sentimentos de injustiça e suscitando perplexidade quanto ao papel da responsabilidade civil” *In*: SCHREIBER, Anderson. **Novos Paradigmas da Responsabilidade Civil**: da erosão dos filtros da reparação à diluição dos danos. São Paulo: Editora Atlas, 2ª ed., 2009. p. 247.

⁹⁷ MULHOLLAND, Caitlin Sampaio. **A responsabilidade civil por presunção de causalidade**. Rio de Janeiro: GZ Editora, 2010.

identificar, em abstrato, situações que se desenrolariam de forma semelhante àquela que está sendo analisada concretamente. Ela também está associada à noção de repartição de riscos, o que significa que a obrigação de reparar danos é situada na própria realização de uma atividade considerada arriscada. Isso é analisado com base na relevância estatística da ocorrência do dano, levando em consideração a probabilidade de que o evento danoso ocorreria em circunstâncias semelhantes.

4.3.3. O dano plurifacetado

O conceito de dano é central no contexto da responsabilidade civil, pois é o elemento essencial que dá origem ao dever de indenizar. Sem a existência de um dano, seja ele patrimonial ou extrapatrimonial, não se cogita a responsabilidade civil, uma vez que não há lesão a ser reparada. Nesse contexto, a noção de dano desempenha um papel fundamental na determinação das obrigações legais e financeiras de uma parte que causou prejuízo a outra.⁹⁸

Conforme conceituado por Carlos Alberto Bittar, o dano pode ser entendido como "*qualquer lesão injusta a componentes do complexo de valores protegidos pelo Direito, incluído, pois, o de caráter moral*"⁹⁹. Isso significa que o dano não se limita apenas a danos materiais ou patrimoniais, mas também engloba danos morais, que dizem respeito à lesão a aspectos não financeiros da pessoa, como sua dignidade, honra, imagem e intimidade.

No entanto, é importante destacar que o dano reparável deve ser injusto. Isso significa que nem toda lesão resulta em um dano indenizável. Por exemplo, não se considera dano injusto quando a lesão é decorrente de uma ação autorizada pelo direito. Nesses casos, fala-se em "*dano justo*". Por exemplo, atos praticados em *legítima defesa* ou no *exercício regular de um direito reconhecido* não configuram dano injusto e, portanto, não dão origem a um dever de indenizar¹⁰⁰.

A consideração do dano como um elemento-chave na responsabilidade civil reflete uma abordagem que vai além dos requisitos tradicionais e enfatiza a importância de avaliar a lesão a interesses protegidos pelo ordenamento jurídico, em nível superior à ilicitude do ato. Esse

⁹⁸ MULHOLLAND, Caitlin Sampaio. **A responsabilidade civil por presunção de causalidade**. Rio de Janeiro: GZ Editora, 2010.

⁹⁹ BITTAR, Carlos Alberto. **Reparação Civil por Danos Morais**. 4. ed., rev., aum. e mod. por Eduardo Carlos Bianca Bittar. São Paulo: Saraiva, 2015. p. 18-19.

¹⁰⁰ BITTAR, Carlos Alberto. **Responsabilidade Civil**. Teoria e Prática. Atualização de Eduardo Carlos Bianca Bittar. 4. ed. Rio de Janeiro: Forense Universitária, 2005. p. 9.

entendimento coloca o dano como o último filtro de contenção de demandas por reparação, dando-lhe um papel central na determinação do dever de indenizar. Essa abordagem se baseia em referenciais valorativos constitucionais e busca identificar quais condutas ensejam a obrigação de reparar.

Conforme destacado por André Ramos¹⁰¹, a ideia de dano reparável se afasta da mera ilicitude do ato e se concentra na lesão a um interesse posicionado em um nível mais elevado na ordem jurídica em relação àquele que orienta a ação lesiva. Isso implica que o dano deixa de ser visto apenas como um elemento estático e pressuposto das ações de responsabilidade civil, tornando-se uma cláusula geral destinada a selecionar os interesses que merecem tutela e cuja violação dá origem ao dever de indenizar.

Essa abordagem reconhece que a reparação não deve ser meramente uma consequência da ilicitude do ato, mas sim uma resposta à lesão efetiva de interesses legalmente protegidos. Portanto, o foco passa a ser a proteção dos interesses prejudicados em vez de apenas a punição da conduta ilícita. Isso permite uma análise mais abrangente e contextualizada dos casos de responsabilidade civil, levando em consideração não apenas a conduta do agente, mas também o impacto real daquela conduta sobre os interesses das vítimas.

Como bem ressaltou Rui Stoco, essa obrigação representa o preço que cada indivíduo deve pagar por viver em sociedade e interagir com seus pares. Ela é uma expressão do princípio fundamental de respeito aos direitos do próximo e da necessidade de agir de acordo com as regras e normas estabelecidas pela sociedade e pelo Direito positivo.¹⁰²

A clássica doutrina categoriza os danos em duas principais vertentes: os patrimoniais e os extrapatrimoniais. De acordo com a definição de Eneas de Oliveira Matos, os danos patrimoniais são aqueles em que ocorre a violação de um bem jurídico que faz parte do patrimônio econômico da vítima, afetando interesses relacionados a questões financeiras e que podem ser avaliados em termos monetários. Por outro lado, os danos extrapatrimoniais são definidos de maneira negativa pelo mesmo autor, englobando todas as situações que não se

¹⁰¹ RAMOS, André Luiz Arnt. A responsabilidade civil para além dos esquemas tradicionais: prospecções do dano reparável na contemporaneidade. **Revista Fórum de Direito Civil - RFDC**. Belo Horizonte, ano 4, n. 10, p. 13-33, set./dez., 2015.

¹⁰² STOCO; Rui. **Tratado de responsabilidade civil: doutrina e jurisprudência**. São Paulo: Editora Revista Dos Tribunais, 2007.

enquadram na categoria de danos patrimoniais, ou seja, aqueles que não resultam diretamente na lesão de um bem jurídico avaliável em termos financeiros.¹⁰³

De se destacar que “o dano é a lesão a um bem jurídico, o qual compreende não só o patrimônio, mas também toda ordem de direitos personalíssimos como a honra, vida, privacidade, proteção de dados, dentre outros”.¹⁰⁴

É importante ressaltar que a evolução da sociedade e a mudança nas percepções sociais e legais levaram ao reconhecimento de novas modalidades de danos, em particular, o dano moral. Anteriormente, a reparação do dano moral era uma questão controversa e limitada. A ideia predominante era que o dano moral só poderia ser reparado se tivesse reflexos diretos no patrimônio da pessoa, o que era um critério restritivo.

Inobstante a isso, com a promulgação da Constituição vigente, o entendimento sobre o dano moral evoluiu significativamente. O artigo 5º, incisos V e X, da Constituição Federal estabeleceu que a intimidade, a honra, a imagem e a vida privada são invioláveis, e assegurou o direito à indenização por danos morais. Isso abriu o caminho para uma interpretação mais ampla e abrangente do dano moral, que não depende mais da necessidade de reflexos patrimoniais.

Atualmente, o Código Civil brasileiro não conceitua o dano moral de forma específica, mas reconhece sua existência e ilicitude no artigo 186 e estabelece o dever de reparação no artigo 927. Essa evolução reflete uma compreensão mais moderna dos direitos individuais e da importância de proteger não apenas o patrimônio financeiro, mas também os direitos pessoais e subjetivos das pessoas.

Frise-se, ademais, que a jurisprudência tem desempenhado um papel fundamental no reconhecimento e na evolução das modalidades de danos no âmbito da responsabilidade civil. Através de decisões judiciais e súmulas, os tribunais têm estabelecido precedentes importantes que moldam a interpretação e a aplicação das leis relacionadas aos danos.

Um exemplo relevante disso é a Súmula nº 37 do Superior Tribunal de Justiça (STJ), que esclareceu a possibilidade de cumulação dos danos materiais e morais decorrentes do

¹⁰³ COUTINHO, Marina de Alencar Araripe. **A proteção da vítima de danos causados por uma inteligência artificial**: uma perspectiva civil-constitucional. Orientador: Prof. Dr. Fabiano Hartmann. 2022. 129 p. Dissertação (Mestrado no curso de Direito) - Universidade de Brasília, Brasília, 2022. p.52.

¹⁰⁴ COUTINHO, Marina de Alencar Araripe. **A proteção da vítima de danos causados por uma inteligência artificial**: uma perspectiva civil-constitucional. Orientador: Prof. Dr. Fabiano Hartmann. 2022. 129 p. Dissertação (Mestrado no curso de Direito) - Universidade de Brasília, Brasília, 2022.

mesmo fato. Essa súmula estabeleceu um importante precedente ao reconhecer a autonomia dos danos morais em relação aos danos materiais, permitindo que ambos fossem pleiteados e compensados em casos de prejuízo. Essa decisão abriu caminho para uma compreensão mais ampla e flexível dos tipos de danos que podem ser objeto de reparação.¹⁰⁵

Além disso, a Súmula 387 do STJ, que trata da autonomia dos danos estéticos em relação aos danos morais, é outro exemplo de como a jurisprudência tem desempenhado um papel crucial no reconhecimento de novas modalidades de danos. Essa súmula estabeleceu que os danos estéticos, que dizem respeito à lesão à aparência física da vítima, podem ser pleiteados separadamente dos danos morais, ampliando ainda mais o escopo de reparação.¹⁰⁶

A evolução na concepção tradicional do modelo de riqueza também desempenhou um papel importante na expansão dos tipos de danos. A compreensão de que a propriedade não se limita apenas a bens corpóreos, mas também abrange bens incorpóreos e intangíveis, demonstra a modificação nos tipos de danos que podem surgir. Muitos desses bens incorpóreos, como a reputação, a privacidade e os dados pessoais, podem ter um valor igual ou superior aos bens materiais.

Com efeito, o debate sobre novas modalidades de danos extrapatrimoniais visa manter atualizado o instituto da responsabilidade civil, garantindo que as vítimas sejam integralmente reparadas por todos os danos sofridos. Em países que seguem a tradição jurídica francesa, o conceito de dano é flexível e aberto, permitindo que qualquer lesão a um interesse lícito seja considerada como ponto de partida para a responsabilidade civil. A análise se dá pela verificação do nexos causal entre o dano e o comportamento culposos ou o risco de uma atividade.¹⁰⁷

Trazendo tais conceitos para o tema sob análise, é de se destacar que os danos advindos dos delitos de usurpação de identidade são uma preocupação crescente na era digital. Abaixo os principais tipos de danos relacionados a esse delito:

¹⁰⁵ COUTINHO, Marina de Alencar Araripe. **A proteção da vítima de danos causados por uma inteligência artificial**: uma perspectiva civil-constitucional. Orientador: Prof. Dr. Fabiano Hartmann. 2022. 129 p. Dissertação (Mestrado no curso de Direito) - Universidade de Brasília, Brasília, 2022.

¹⁰⁶ COUTINHO, Marina de Alencar Araripe. **A proteção da vítima de danos causados por uma inteligência artificial**: uma perspectiva civil-constitucional. Orientador: Prof. Dr. Fabiano Hartmann. 2022. 129 p. Dissertação (Mestrado no curso de Direito) - Universidade de Brasília, Brasília, 2022.

¹⁰⁷ MONTEIRO FILHO, Carlos Edison do Rêgo; ROSENVALD, Nelson. **Danos causados a dados pessoais: novos contornos**. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/332618/danos-causados-a-dados-pessoais--novos-contornos> - Acesso em: 21 set. 23.

Tabela 4: Principais tipos de danos relacionados à usurpação de identidade

Dano Financeiro	Uma das consequências mais imediatas da usurpação de identidade é o dano financeiro. Os criminosos podem usar informações pessoais roubadas, como números de cartão de crédito, senhas bancárias ou dados fiscais, para realizar transações fraudulentas, abrir contas bancárias em nome da vítima ou solicitar empréstimos e crédito, causando prejuízos financeiros substanciais.
Dano à Reputação	Os criminosos podem, ainda, usar a identidade da vítima para cometer crimes, enviar mensagens difamatórias, ou envolver-se em atividades ilegais. Isso pode levar a vítima a ser erroneamente associada a essas atividades prejudiciais, afetando sua reputação pessoal e profissional.
Dano Legal	Muitas vítimas de usurpação de identidade enfrentam desafios legais. Eles podem ser erroneamente implicados em atividades ilegais, o que pode resultar em investigações policiais, detenções e até mesmo acusações criminais injustas.
Dano à Privacidade	A usurpação de identidade envolve a invasão da privacidade da vítima, já que informações pessoais e sensíveis são apropriadas e utilizadas sem autorização.
Dano Social	A exposição pública de informações pessoais, especialmente em plataformas online, pode causar danos sociais. Isso pode incluir a disseminação de informações pessoais ou íntimas, levando a vítima a enfrentar estigma ou discriminação.

Portanto, o dano é um elemento essencial na fundamentação do dever de reparação na responsabilidade civil e, para que seja considerado como tal, deve atender a certos critérios e características. Estes critérios ajudam a determinar a elegibilidade do dano para fins de indenização e garantem a justiça e a equidade no processo de reparação.

4.3.5. O dano moral e o Titular de Dados Pessoais

É sabido que a Lei Geral de Proteção de Dados (LGPD) representa um avanço significativo na regulamentação da proteção de dados pessoais no Brasil. Ocorre que referida lei não fornece diretrizes específicas sobre a natureza dos danos que podem surgir em casos de

violações de dados pessoais. Em vez disso, deixa a critério dos magistrados avaliar se os danos são de natureza material ou moral, e se são considerados "*in re ipsa*" (danos presumidos) ou não.

Um exemplo relevante é quando se trata de violações de dados que envolvem a exposição não autorizada de informações pessoais sensíveis, como vazamento de fotografias íntimas armazenadas na nuvem por um provedor de serviços. Nestes casos, os danos morais podem ser presumidos, uma vez que a exposição de informações íntimas sem consentimento claramente viola a privacidade do indivíduo e pode causar sofrimento emocional.

Por outro lado, existem situações em que a violação de dados pode não resultar em danos imediatos ou facilmente identificáveis. Por exemplo, no caso de vazamento de *logs* que, embora possam tornar o titular de dados identificável, não o identificam prontamente e não podem ser facilmente usados para prejudicá-lo. Nesses casos, a determinação dos danos pode ser mais complexa e dependerá de fatores específicos do caso.

No âmbito cível, já existem decisões judiciais que abordam a questão dos danos ou da falta deles em casos de supostas violações à legislação de proteção de dados. Por exemplo, o Tribunal de Justiça de São Paulo já decidiu que é necessário que o consumidor comprove os danos decorrentes do vazamento de dados pessoais. Isso significa que, para buscar uma compensação por danos morais ou materiais, o consumidor deve demonstrar que sofreu prejuízos reais como resultado da violação de dados.

Ação de obrigação de fazer c.c. indenização por danos morais. Vazamento de dados pessoais. Sentença de improcedência. Apelação do autor. Vazamento de dados pessoais. Falha na prestação de serviço. Dever da empresa de adotar medidas de segurança visando à proteção de dados pessoais do consumidor. Inteligência do artigo 46 da Lei Geral de Proteção de Dados (Lei n.º 13.709/2018). Danos morais não verificados. Vazamento de dados que não ensejou dano efetivo ao requerente. Dados vazados que não estão abrangidos no conceito de dado pessoal sensível (art. 5º, II, da LGPD). Ausência de prova acerca da utilização dos dados vazados e do efetivo dano. Dano hipotético não enseja indenização. Precedentes do TJSP. Sentença mantida. Honorários majorados. Recurso desprovido.¹⁰⁸

Igualmente é o posicionamento estabelecido pela Segunda Turma do Superior Tribunal de Justiça (STJ) ao dar provimento ao Recurso Especial (REsp) da Eletropaulo. Em seu voto, o ministro relator, Francisco Falcão, também afirmou que, no caso dos autos, o dano moral não é

¹⁰⁸ TJSP; **Apelação Cível 1001032-45.2021.8.26.0177**; Rel. Virgílio de Oliveira Junior; Órgão Julgador: 23ª Câmara de Direito Privado; Foro de Embu-Guaçu, Vara Única, j. 01/12/2021; Registro 03/12/2021

presumido, sendo necessário que o titular dos dados demonstre ter havido efetivo dano com o vazamento e o acesso de terceiros.

"Diferente seria se, de fato, estivéssemos diante de vazamento de dados sensíveis, que dizem respeito à intimidade da pessoa natural. No presente caso, trata-se de inconveniente exposição de dados pessoais comuns, desacompanhados de comprovação do dano"¹⁰⁹

A complexidade e a falta de uniformidade na avaliação dos danos em casos de violação de dados pessoais refletem os desafios enfrentados pelos tribunais ao lidar com um campo jurídico em constante evolução. A proteção de dados pessoais é uma questão contemporânea e complexa que envolve uma série de fatores, incluindo tecnologia, privacidade e direitos individuais.

Nesse contexto, a jurisprudência desempenha um papel fundamental na definição das regras e padrões que regem esses casos. Enquanto isso, a conscientização acerca da importância da proteção de dados e da privacidade é fundamental para todas as partes envolvidas. Isso inclui, principalmente, os consumidores, que devem estar cientes de seus direitos e tomar precauções para proteger suas informações pessoais.

Resta-nos, diante do exposto, perceber qual é o grau de lesão do bem jurídico atingido em casos de usurpação de identidade.

A diferenciação entre obtenção e uso de dados desempenha um papel importante na avaliação do grau de lesão. Quando alguém obtém dados, o rastro informático é geralmente menor do que quando esses dados são efetivamente usados de maneira criminosa. O uso de dados envolve uma conduta ativa e contínua por parte do agente, como no caso de um esquema de *catfishing*, no qual o agente mantém um perfil online falso para enganar outra pessoa. Nesse contexto, a vulnerabilidade da vítima aumenta à medida que a ação criminosa prossegue.

De toda sorte, a maioria dos agentes que praticam esse tipo de crime busca causar prejuízos patrimoniais, como evidenciado por estudos internacionais que demonstram perdas anuais relacionadas à utilização indevida de dados de terceiros.

¹⁰⁹ STJ; AREsp nº 2130619 / SP (2022/0152262-2); Rel. Francisco Falcão; Órgão Julgador: 2ª Turma do Superior Tribunal de Justiça; j. 07/03/2023.

Portanto, a discussão gira em torno da possibilidade de haver um dever autônomo de reparação para essa conduta criminosa (obtenção indevida), mesmo antes de ocorrer uma lesão efetiva ao bem jurídico (utilização indevida).

E quanto a esse ponto, como se viu, a análise legal e jurisprudencial está em evolução, buscando encontrar um equilíbrio entre a proteção dos direitos individuais e a avaliação adequada dos danos causados por crimes de usurpação de identidade. A tendência é de que o próprio titular de dados comprove a efetiva lesão à personalidade, o que torna sua aplicação ainda muito subjetiva. De todo modo, a legislação e a jurisprudência continuarão a se desenvolver à medida que mais casos forem apresentados e decisões forem proferidas, e a questão da natureza dessa reparação será continuamente revisada e interpretada.

4.3.6. A culpa e o risco no regime de responsabilidade

Como visto, a teoria da responsabilidade subjetiva é um dos pilares do sistema jurídico que determina quando e como um agente pode ser responsabilizado por seus atos. Nessa abordagem, o comportamento do agente desempenha um papel central na avaliação de sua responsabilidade. É crucial que o agente tenha agido de forma culposa, ou seja, ele deve ter se comportado de maneira contrária ao que o ordenamento jurídico lhe exige. Isso implica agir com cautela, prudência, vigilância, perícia, cuidado e de acordo com os padrões de conduta aplicáveis à sua atividade.

Rui Stoco destaca a importância de acrescentar um "juízo de reprovação" baseado na culpabilidade. Esse juízo considera o dolo, que envolve a vontade dirigida a um fim, e a culpa em sentido estrito, que engloba imprudência, negligência e imperícia¹¹⁰. Ou seja, a culpa é um elemento fundamental na análise da responsabilidade subjetiva, e a conduta negligente ou imprudente do agente pode resultar em sua responsabilização.

No entanto, Stoco também observa que, devido à dinâmica dos fatos e à evolução da disciplina da responsabilidade civil, pode surgir a responsabilidade sem culpa. Isso ocorre, por exemplo, por força da teoria do risco ou quando a lei não exige a comprovação de ilicitude. Essa perspectiva amplia o escopo da responsabilidade civil para além da culpa do agente,

¹¹⁰ STOCO; Rui. **Tratado de responsabilidade civil: doutrina e jurisprudência**. São Paulo: Editora Revista Dos Tribunais, 2007. p. 113.

reconhecendo que, em certas situações, a responsabilidade pode surgir independentemente da conduta culposa.¹¹¹

Na obra "Novo Tratado de Responsabilidade Civil", Farias, Braga Netto e Rosenvald destacam o nexo de imputação como um novo pressuposto da responsabilidade civil. Esse nexo, também conhecido como fator de atribuição, refere-se às razões legais ou contratuais que permitem atribuir o dever de indenizar a alguém quando ocorre um dano injusto. O entendimento desse nexo de imputação é crucial para o estudo das causas excludentes de responsabilidade civil, pois muitas vezes a natureza subjetiva ou objetiva da responsabilidade é determinada com base na previsão das excludentes no texto legal.¹¹²

4.4. A DIMENSÃO OBJETIVA DA CONDUTA DA VÍTIMA DE FRAUDES

O estudo da vitimologia desempenha um papel crucial na compreensão dos fatores que influenciam a ocorrência de delitos e na análise da dinâmica entre vítimas e delinquentes. Nesse mesmo diapasão, a análise da conduta da vítima de crimes cibernéticos desempenha um papel importante na mensuração da responsabilidade civil em casos envolvendo violações digitais. Isso porque ela ajuda a determinar se a vítima tomou medidas razoáveis de segurança, compreendeu os riscos envolvidos e agiu com prudência no ambiente digital. Essa análise contribui para a justa atribuição de responsabilidade e para a promoção da segurança cibernética.

À medida que a pesquisa nessa área evolui, torna-se cada vez mais evidente que diversos elementos, como a personalidade da vítima, sua situação de vida, educação, habilidade para antecipar riscos, perspectiva da realidade e ambientes frequentados, desempenham um papel fundamental no cometimento de um crime e na criação de sua própria ecologia.¹¹³

O ato criminoso não é um evento isolado, mas composto por estágios que antecedem, envolvem e sucedem a ação criminosa. Os criminosos frequentemente adotam métodos para evitar a identificação futura de sua autoria, caso haja consequências legais. Nesse contexto, a compreensão da vítima potencial torna-se ainda mais relevante, uma vez que a análise desses

¹¹¹ STOCO; Rui. **Tratado de responsabilidade civil: doutrina e jurisprudência**. São Paulo: Editora Revista Dos Tribunais, 2007.

¹¹² BRAGA NETTO, Felipe Peixoto; FARIAS, Cristiano Chaves; ROSENVALD, Nelson. **Novo Tratado de Responsabilidade Civil**. 3. ed. São Paulo: Saraiva Educação, 2018. p. 595.

¹¹³ SYDOW, 2009.

fatores pode fornecer *insights* sobre como os criminosos escolhem suas vítimas e planejam suas ações.

No cenário contemporâneo, em que a interatividade dos sistemas informáticos desempenha um papel central, as consequências no ciberespaço frequentemente são desencadeadas por ações da própria vítima. Isso ocorre porque a postura e o comportamento de indivíduos online podem influenciar diretamente sua exposição a riscos cibernéticos. No entanto, é importante destacar que isso não visa isentar o vitimário de sua responsabilidade ao violar o bem jurídico alheio. Em vez disso, destaca-se a necessidade de compreender o cruzamento lógico entre a atitude tomada pelas vítimas no ciberespaço e a atitude adotada pelos ofensores.

Nesse sentido, a conscientização sobre as melhores práticas de segurança online, a educação sobre como reconhecer ameaças e a promoção de comportamentos responsáveis no ciberespaço são medidas cruciais para reduzir a incidência de crimes cibernéticos. Além disso, a compreensão das motivações dos criminosos e a análise dos fatores que tornam alguém mais vulnerável a ataques cibernéticos podem contribuir para uma abordagem mais abrangente e eficaz na prevenção e combate a crimes no mundo digital.

A tecnologia da informação, embora muitas vezes seja associada à ideia de anonimato, não foi projetada para a impunidade. A afirmação de que a virtualidade oferece uma forma segura e impune de cometer atos delinquentes não é verdadeira, pois a navegação, o acesso e o uso de programas deixam rastros, o que torna possível rastrear aqueles que utilizam o ambiente digital para atividades criminosas.

A rastreabilidade no mundo digital é um conceito importante. Mesmo que os atores criminosos tentem ocultar sua identidade, muitas vezes deixam vestígios que podem ser usados para identificá-los. Isso é fundamental para a aplicação da lei e a responsabilização daqueles que cometem crimes online.

Além disso, os criminosos podem criar códigos programados para lesar o bem jurídico de terceiros. Eles desenvolvem programas maliciosos que se autoexecutam nos dispositivos de suas vítimas, mas geralmente exigem permissão do usuário para fazê-lo. Como se viu, os vitimários também podem criar páginas com conteúdo enganoso, como imagens eróticas, fotografias de acidentes ou delitos, links que prometem downloads de músicas, mas que, na realidade, instalam códigos maliciosos nos dispositivos das vítimas. Isso ressalta a importância da conscientização e da educação digital para se proteger contra ameaças cibernéticas.

Justamente por esta razão, entende-se que para combater eficazmente os delitos informáticos, é fundamental estabelecer uma linha clara em relação à conduta da vítima. Nesse sentido, apregoa Cancio Meliá¹¹⁴ que quatro são as ideias a serem consideradas na construção dogmática do impacto do comportamento da vítima:

- a) O raciocínio da *concorrência de culpas* e do *dever objetivo de cuidado* por parte das vítimas destaca a responsabilidade compartilhada entre as partes envolvidas em um crime. Isso implica que as vítimas também têm a obrigação de tomar precauções razoáveis para proteger seus próprios interesses.
- b) A ideia de que a vítima deve ter assumido conscientemente sua postura e compreendido a extensão de seu consentimento enfatiza a importância da consciência e da compreensão por parte da vítima em relação às ações que está realizando no ambiente digital.
- c) A distinção entre *autocolocação da vítima em risco* e *heterocolocação da vítima em risco* consentida considera se a vítima colocou a si mesma em risco ou se foi colocada em risco por ações de terceiros, mas consentiu nessa exposição ao risco.
- d) O raciocínio vitimodogmático de merecimento de proteção, estabelecendo o "*Princípio vitimológico*", implica que a extensão da responsabilidade do autor deve ser medida em relação à responsabilidade de autoproteção da vítima. Isso significa que as vítimas têm a responsabilidade de tomar medidas para proteger seus próprios interesses.

Assim, a assunção de que há uma quantidade de responsabilidade por parte de todos os atores do crime, incluindo as vítimas, destaca a importância da prevenção e da autoproteção no mundo digital. Todos os envolvidos têm a obrigação de respeitar os bens jurídicos uns dos outros, e as vítimas devem tomar precauções mínimas necessárias para evitar exposição a riscos excessivos e desnecessários. Essa abordagem holística é fundamental para promover um ambiente digital mais seguro e responsável.

Com efeito, há que se considerar que o conceito de responsabilidade da vítima em delitos é complexo e requer uma análise cuidadosa de vários pontos. Para entendermos melhor o âmbito de responsabilidade da vítima, Sidow¹¹⁵ destaca que é importante considerar os seguintes pontos:

Tabela 5: Parâmetros a serem considerados na análise da responsabilidade do ofendido.

Organização conjunta entre autor e vítima.	Em algumas situações, a atividade delincente pode ser organizada conjuntamente entre o autor do crime e a vítima. Isso significa que ambos estão envolvidos na ação criminosa
---	---

¹¹⁴ MELIÁ, Manuel Cancio. **Conducta de la víctima e imputación objetiva en derecho penal:** estudio sobre los ámbitos de responsabilidad de víctima y autor en actividades arriesgadas. Bogotá: Universidad Externado De Colombia, 2001, pp. 91-92.

¹¹⁵ SYDOW, Spencer Toth. **Delitos informáticos próprios:** uma abordagem sob a perspectiva vitimodogmática. Orientador: Sergio Salomão Shecaira. 2009. Dissertação (Mestrado no curso de Direito) - Universidade de São Paulo, São Paulo, 2009. p.212.

	de forma colaborativa. Nesse caso, a responsabilidade da vítima pode ser inquirida porquanto ela participa ativamente do crime.
Conduta da vítima não instrumentalizada pelo autor	A responsabilidade da vítima não deve ser aplicada quando sua conduta é instrumentalizada pelo autor do crime. Se a vítima não possui base cognitiva para agir de forma independente e consciente, não pode ser considerada auto responsável pela sua participação na ação criminosa.
Ausência de dever de proteção específico do autor	Além disso, a responsabilidade da vítima pode ser questionada se o autor do crime não tiver um dever de proteção específico em relação aos bens da vítima. Ou seja, se o autor não for o guardião ou responsável direto pela segurança dos bens violados, a responsabilidade recai menos sobre a vítima.

A mensuração do grau de consciência da vítima em relação às suas ações é fundamental nesse contexto. Se a vítima reconhece conscientemente o aumento do risco, ou se esse aumento é presumido, ela pode ser considerada inescusável em suas ações. A teoria da ação jurídica, como defendida por Bierling¹¹⁶, enfatiza que os bens jurídicos são tutelados pelo direito apenas se seus titulares os consideram valiosos. Portanto, se a vítima permite conscientemente a ofensa, pode-se argumentar que o Estado não precisa tutelar juridicamente esses bens, o que reforça a ideia de um "Princípio vitimodogmático".

Para uma compreensão mais profunda dessas ideias, é importante explorar os conceitos de consentimento do ofendido e autocolocação da vítima em risco. O primeiro conceito diz respeito à concordância ou permissão da vítima em relação à ação criminosa, enquanto o segundo se relaciona à decisão da vítima de se colocar em uma situação de risco sem coerção externa.

¹¹⁶ “Em derradeiro, merece atenção a concepção tecida por Mezger ao expender um aprimoramento a teoria de Bierling, asseverando que o consentimento pressupõe “o abandono consciente dos interesses por parte daquele que, legitimamente, tem a faculdade de disposição sobre o bem jurídico” *In*: PIERANGELI, José Henrique. **O Consentimento do Ofendido na Teoria do Delito**. 3ª Edição revista e atualizada. São Paulo: Editora Revista dos Tribunais. 2001. p. 79.

4.4.1. Consentimento do Lesado

A inclusão do consentimento do lesado como uma causa excludente de ilicitude é um importante aspecto do direito civil em diversos sistemas jurídicos. No Código Civil Português, o consentimento do prejudicado é claramente estabelecido como uma exceção à ilegalidade, conforme indicado no artigo 340º:

ARTIGO 340º

(Consentimento do lesado)

1. O acto lesivo dos direitos de outrem é lícito, desde que este tenha consentido na lesão.
2. O consentimento do lesado não exclui, porém, a ilicitude do acto, quando este for contrário a uma proibição legal ou aos bons costumes.
3. Tem-se por consentida a lesão, quando esta se deu no interesse do lesado e de acordo com a sua vontade presumível.¹¹⁷

O Código Civil Argentino explicita que o consentimento do prejudicado é considerado uma causa de justificação, conforme estabelecido no artigo 1720 do supra:

ARTIGO 1720.

Consentimento do lesado

Sem prejuízo de disposições especiais, o consentimento livre e esclarecido do lesado, na medida em que não constitua cláusula abusiva, exime de responsabilidade pelos danos decorrentes da lesão aos bens disponíveis.¹¹⁸

A ausência de uma menção expressa ao consentimento como causa excludente de ilicitude no Código Civil brasileiro é uma característica notável em comparação com o Código Civil português e o Código Civil argentino. No entanto, mesmo que o código brasileiro não faça essa menção explícita, o entendimento do consentimento como uma causa excludente de ilicitude tem sido aceite e aplicado com base na análise lógica dos pressupostos da responsabilidade civil.

Francisco Amaral destaca o conceito de "*volenti non fit injuria*" (aquele que consente não sofre dano) como uma base para a compreensão do consentimento do ofendido como excludente de ilicitude. Amaral explica que quando o prejudicado consente na lesão a seu

¹¹⁷ Código Civil Português. **Decreto-Lei nº 47344/66**. Diário da República Eletrónico. Disponível em: <https://dre.pt/web/guest/pesquisa/-/search/477358/details/normal?l=1> – Acesso em: 22 set. 23

¹¹⁸ Tradução do seguinte trecho no original: “*ARTÍCULO 1720. Consentimiento del damnificado. Sin perjuicio de disposiciones especiales, el consentimiento libre e informado del damnificado, en la medida en que no constituya una cláusula abusiva, libera de la responsabilidad por los daños derivados de la lesión de bienes disponibles.*” Disponível em: <https://www.argentina.gob.ar/normativa/nacional/ley-26994-235975>. Acesso em: 22 set. 23

próprio direito, não há ilegalidade no comportamento do agente e, portanto, o dano não é indenizável.¹¹⁹

Esse princípio é frequentemente aplicado em situações como competições esportivas, em que os participantes aceitam o risco inerente às atividades esportivas, a menos que haja uma manifesta intenção de causar dano. Isso significa que lesões acidentais que ocorrem em um contexto esportivo podem não ser consideradas ilícitas.

Outro exemplo notável é o consentimento como causa excludente de ilicitude especial no âmbito do dever de sigilo bancário, conforme estabelecido no §3º, inciso V, da Lei Complementar nº 105/2001, conhecida como a Lei de Sigilo Bancário. Isso indica que, sob certas circunstâncias e dentro do contexto regulatório adequado, o consentimento pode justificar a quebra do sigilo bancário.

Portanto, o consentimento do indivíduo pode ser considerada uma excludente geral de antijuridicidade ou ilicitude, em consonância com o respeito à sua autonomia de vontade, apenas se (i) o indivíduo tenha a capacidade necessária para discernir, (ii) a situação a ser consentida esteja dentro de sua esfera de disponibilidade, ou seja, sem infringir sua dignidade humana, direitos de terceiros, o interesse público, os costumes e (iii) não haja proibição legal, inclusive no contexto penal.¹²⁰

É importante observar que na doutrina jurídica existe um consenso de que os bens que permitem o consentimento para sua ofensa são predominantemente aqueles de natureza patrimonial e personalíssima, essencialmente disponíveis, e que não afetam valores difusos.

No entanto, certas condutas, como intrusão informática, usurpação de identidade, crimes contra a honra, entre outros, podem ter como alvo um bem jurídico que já está explícito na ordem penal ou a segurança telemática e podem ter incidência e potencial de prejuízo exclusivamente individual. Nesses casos, os bens jurídicos afetados podem ser considerados disponíveis, o que dá margem à possibilidade de violação consentida.

A adaptação da ideia de consentimento do ofendido ao ambiente peculiar da internet e das redes de computadores é um tema complexo que levanta questões importantes sobre a responsabilidade e a aplicação desse princípio. Muitos delitos cibernéticos ocorrem sem o

¹¹⁹ AMARAL, Francisco. **Direito Civil**: introdução. 10. ed. revista e modificada. São Paulo: Saraiva Educação, 2018. p. 645.

¹²⁰ como exemplificado nas seguintes exceções ao consentimento como causa de exclusão de ilegalidade: (a) restrições ao direito de propriedade em conformidade com sua função social; (b) incitação, estímulo ou auxílio ao suicídio ou automutilação, inclusive online; (c) aborto consentido; (d) eutanásia voluntária; entre outros casos.

conhecimento direto do usuário lesado, que pode ter seu sistema invadido e suas informações comprometidas por agentes criminosos. Surge, então, a pergunta: seria possível considerar que, ao não adotar as precauções conhecidas para a segurança de seu sistema informático, a vítima indiretamente consente com a conduta prejudicial a si mesma?

Spencer¹²¹ entende que não. A maioria dos casos não envolve um consentimento explícito, mas sim uma invasão decorrente de um descuido, omissão ou negligência do usuário. No cenário mencionado, em que ocorre uma intrusão informática com o único propósito de superar as barreiras de segurança do dispositivo de um usuário e acessar seus dados, está ocorrendo uma violação do bem jurídico específico, que é o computador e as informações contidas nele.

A particularidade do consentimento do ofendido reside no fato de que o consentidor deve aceitar conscientemente os riscos e os resultados de sua ação, demonstrando sua disponibilidade de forma expressa ou implícita. Isso deve ser feito a tal ponto que o agente ofensor tenha a certeza de que não há interesse em proteger aquele bem jurídico, dentro dos limites morais e sem prejudicar outros direitos de terceiros ou interesses coletivos. Portanto, há um elemento volitivo por parte daquele que renuncia ao seu próprio bem jurídico.

A teoria subjetiva apresentada por Pierangeli argumenta que a presunção de consentimento exige não apenas os elementos tradicionais do consentimento (disponibilidade do bem, consciência para dispor e voluntariedade), mas também a capacidade de prever prognosticamente se o titular do direito consentiria com a violação se tivesse conhecimento da situação prejudicial ao bem em questão.

Nesse contexto, acredita-se que mesmo quando o usuário não tenha adotado medidas de segurança adequadas para proteger seu dispositivo tecnológico ele não deveria ser considerado como alguém que aceitou que a confidencialidade, integridade ou disponibilidade de seu sistema fosse violada, dada a importância desses bens em seu dia a dia.

Além disso, a ideia de que a vítima deve suportar a perda do direito não se aplica facilmente aos crimes informáticos. Em muitos casos, a falta de cuidado por parte do lesado resulta em arrependimento posterior, mas muitas vezes o prejuízo sofrido não pode ser

¹²¹ SYDOW, Spencer Toth. **Delitos informáticos próprios**: uma abordagem sob a perspectiva vitimodogmática. Orientador: Sergio Salomão Shecaira. 2009. Dissertação (Mestrado no curso de Direito) - Universidade de São Paulo, São Paulo, 2009. p.215.

revertido, especialmente quando se trata de dados digitais cujo valor não pode ser equiparado ao de objetos materiais.

Assim, conclui-se que a atitude da vítima em relação aos crimes informáticos pode ser considerada como uma verdadeira causa de exclusão de ilicitude quando há uma permissividade em relação à violação de um dos bens envolvidos nos crimes informáticos. No entanto, como regra geral, a prática comum na internet envolve a exploração de vulnerabilidades nos sistemas informáticos, mas não implica que o usuário imprudente tenha aceitado conscientemente o resultado prejudicial ou tenha contribuído de forma deliberada para a ocorrência do delito. No entanto, é importante considerar essas omissões e imprudências ao avaliar a responsabilidade do agente criminoso, graduando a quantidade de contribuição dada pela vítima para determinar adequadamente a condenação das partes envolvidas na perfectibilização do crime.

4.4.2. Autocolocação da Vítima em Risco

O conceito de vitimologia, conforme definido por Raul Goldstein¹²², oferece uma perspectiva fundamental na compreensão do sistema legal e das dinâmicas envolvendo vítimas e infratores. A vitimologia vai além de considerar a vítima como mera consequência de uma conduta criminosa, destacando seu papel como uma das causas que influenciam a ocorrência de um crime.

Uma implicação importante dessa perspectiva é que, em determinadas situações, a atenção do operador do direito deve se voltar para a vítima, a fim de avaliar a culpabilidade do infrator de maneira justa e adequada. Isso significa reconhecer que a vítima pode desempenhar um papel ativo nas circunstâncias que levaram ao crime, inclusive por consentimento, tácito ou expresso, em relação a um direito disponível seu, hipótese abordada no tópico anterior.

Como vimos, o consentimento do ofendido pode ser considerado uma causa supralegal de exclusão de ilicitude que reconhece a importância da liberdade da vítima para tomar decisões sobre seus direitos individuais. Ele pressupõe que a vítima tenha a capacidade de tomar uma decisão informada e voluntária sobre abdicar de um direito. Dois elementos fundamentais subjacentes ao consentimento do ofendido são a liberdade de escolha – significa que a vítima

¹²² A vitimologia estuda a vítima não como efeito consequente da realização de uma conduta delitiva, mas como uma das causas, às vezes a principal, que influenciam na produção de um delito. *In*: GOLDSTEIN, Raúl. Diccionario de Derecho Penal y Criminologia *apud*. MOREIRA FILHO, Guaracy. **Vitimologia – O papel da Vítima na Gênese do Delito**. Editora Jurídica Brasileira, São Paulo, 2004. p. 48.

não está sendo coagida, manipulada ou pressionada de qualquer forma a conceder seu consentimento – e a verdadeira disposição da vítima – implica que a vítima deva estar ciente das consequências de abdicar de seu direito e tomar a decisão de maneira consciente.

No entanto, uma lacuna evidente surge com a questão do consentimento do ofendido, o que levanta algumas questões intrigantes no âmbito da apuração do nexo causal. Essa lacuna, identificada e explorada pelo funcionalismo (no direito penal) com base nas teorias de risco desenvolvidas, diz respeito a situações em que a vítima age de forma consciente e livre, resultando em consequências que nem sempre são desejadas por ela, e que podem não ser causadas por terceiros.

Um dos exemplos mais destacados é quando dois indivíduos estão envolvidos no uso de drogas, e um deles morre de overdose. Nesse cenário, é claro que o falecido estava ciente dos riscos associados ao uso excessivo de drogas e, com seu comportamento, acabou provocando sua própria morte, mesmo que não tenha tido a intenção de alcançar esse resultado. Nesse caso, a vítima não deu seu consentimento para a prática de ações prejudiciais a ela, mas estava ciente dos riscos e, por sua própria vontade, se expôs a comportamentos prejudiciais.

É nesse contexto que a teoria da causalidade busca se adaptar, enfrentando o desafio de lidar com situações em que a vítima, agindo de forma consciente e voluntária, contribui para os resultados lesivos, mesmo que não tenha sido diretamente influenciada por terceiros.

O conceito de "autocolocação da vítima em risco" desempenha um papel crucial no sistema jurídico ao modular a culpabilidade de todas as partes envolvidas em um evento danoso. Ele se baseia em certos critérios essenciais que incluem a imputabilidade da vítima, o pleno conhecimento da situação de risco, a disponibilidade do bem em questão e a colaboração total ou parcial da vítima na criação do resultado prejudicial. Quando esses elementos estão presentes, fica claro que a vítima estava em um estado de autocolocação em risco.

O principal objetivo deste instituto é ajustar adequadamente o grau de culpabilidade de cada indivíduo envolvido no evento. Isso é feito considerando princípios legais fundamentais, como o princípio da proporcionalidade e da razoabilidade. Esses princípios visam permitir que os cidadãos assumam uma "margem de responsabilidade com relação à proteção do bem jurídico que depende diretamente da vítima."¹²³

¹²³ GRECO, Alessandra Orcesi Pedro. **A Autocolocação da Vítima em Risco**. São Paulo: Editora RT, 2004. p.115.

Em paralelo com as ideias funcionalistas desenvolvidas por Roxin no Direito Penal, é necessário pressupor a existência de riscos admissíveis na vida em sociedade, ao mesmo tempo em que se reconhecem riscos reprováveis. Isso envolve um raciocínio político-criminal essencial para estabelecer graus de intensidade em relação às ações individuais. Ou seja, há uma expectativa de que as pessoas usem os meios disponíveis para proteger seus próprios bens jurídicos, permitindo que o Estado concentre seus esforços na proteção daqueles que são mais difíceis de preservar.

Destaque-se que, de forma alguma, com a vertente da autocolocação em risco, se está a afirmar que a vítima deseje ativamente sofrer danos, que ela queira que o risco resulte em consequências prejudiciais para si ou que consinta com a violação de seus direitos. Em vez disso, o que se destaca é a noção de uma aceitação eventual ou uma tolerância implícita a possíveis situações lesivas que podem surgir como resultado da criação de um autorrisco.

A criação desse autorrisco ocorre quando a vítima, por meio de suas ações, comportamento ou decisões, gera para si mesma a possibilidade de se tornar alvo de consequências danosas. Essas consequências danosas podem se desdobrar de duas maneiras distintas:

Tabela 6: Hipóteses de criação do Autorrisco pelo ofendido

Causação integral pelo ofendido	Nesse cenário, a vítima, devido a suas ações ou omissões, é diretamente responsável por causar as consequências prejudiciais a si mesma. Isso significa que os danos resultam inteiramente de suas próprias escolhas ou comportamento, mesmo que não tenha a intenção de sofrer tais danos
Facilitação da situação de risco elevado	Em algumas situações, a vítima pode não causar diretamente o dano, mas sua conduta cria uma situação de risco significativamente elevado que facilita a ação de um infrator. Nesse caso, a vítima não é a causa direta das consequências prejudiciais, mas sua ação ou inação contribui para a ocorrência do dano.

É importante ressaltar que esse conceito não absolve, de antemão, o vitimário de sua responsabilidade, mas busca uma compreensão mais completa e equitativa das circunstâncias que cercam o evento, levando em conta a participação da vítima na criação do autorrisco.

O conceito de "papéis sociais" na teoria de Günther Jakobs¹²⁴ desempenha uma função importante ao abordar as responsabilidades tanto dos potenciais infratores quanto das potenciais vítimas dentro de uma sociedade. Jakobs argumenta que, da mesma forma que se espera que aqueles inclinados a cometer crimes não ultrapassem os estágios internos para cometer delitos, também se espera que as possíveis vítimas se mantenham em estágios ótimos de autopreservação. Isso implica não ser aceitável nem que um indivíduo crie intencionalmente riscos para si mesmo, nem que a vítima gere ou aumente riscos, facilitando assim a ocorrência de um delito ou a violação de um bem jurídico indisponível. Ou seja, tanto os potenciais infratores quanto as possíveis vítimas têm responsabilidades sociais a cumprir.

Por esta lógica, Jakobs destaca que cada indivíduo na sociedade tem a obrigação de desempenhar seu papel na prevenção pessoal, contribuindo assim para a formação de um coletivo preventivo. Isso significa que há expectativas sociais em relação a todos aqueles sob a proteção da lei, mesmo porque seria impossível para o Estado supervisionar todas as ações e atitudes de cada membro da sociedade, sobretudo na sociedade de risco potencializada pelo aprimoramento das tecnologias. Isso reflete, ademais, a noção de que a segurança, pessoal ou pública, é uma responsabilidade compartilhada por todos os membros da sociedade.

A abordagem dos papéis sociais destaca a importância da prevenção e da responsabilidade pessoal, mas deve ser aplicada de maneira sensata e justa, levando em consideração as circunstâncias individuais de cada caso.

No contexto da usurpação de identidade pessoal digital, a situação apresenta semelhanças significativas com as questões discutidas anteriormente. À medida que a sociedade evolui em direção a uma sociedade informacional, em que a tecnologia da informação desempenha um papel central, surgem novas dimensões de segurança jurídica. Conforme expõe Sidow, a sociedade informacional no âmbito da informática é uma extensão "*sui generis*" da sociedade, criando um novo bem jurídico, denominado "segurança informática" que se subdivide em aspectos privados – envolvendo questões como a integridade, a confidencialidade ou a disponibilidade de informações que atingem exclusivamente um indivíduo – e aspectos

¹²⁴ JAKOBS, Günther. **A Imputação Objetiva no Direito Penal** (tradução André Luis Callegari), 2ª Edição. São Paulo: Editora Revista dos Tribunais, 2014. pp. 56-74.

públicos – no caso de violações que importam em prejuízo ao meio ambiente informático e que impactam em uma coletividade de pessoas.¹²⁵

Portanto, a figura da autocolocação da vítima em risco, do ponto de vista funcionalista, desempenha um papel crucial na interpretação e aplicação da lei penal. Ela é considerada um elemento subjetivo do tipo, ou seja, influencia a forma como a participação da vítima é avaliada na conduta criminosa, e em alguns casos, pode até mesmo tornar a conduta não passível de enquadramento como crime.

Inobstante a isso, e considerando a subsidiariedade da lei penal, é importante reconhecer que dentro do contexto da responsabilização civil perante uma conduta delituosa a abordagem da autocolocação da vítima em risco também tem implicações significativas. A análise cuidadosa das circunstâncias individuais de cada caso, com atenção às contribuições da vítima e de terceiros, pode ajudar a determinar a extensão da responsabilidade civil em situações envolvendo condutas delituosas, proporcionando uma abordagem justa e equilibrada para a resolução de conflitos.

Justamente por isso, mostra-se pertinente aplicar esse conceito ao escopo deste estudo, destacando que a autocolocação da vítima em risco se baseia nas seguintes premissas: a) a vítima não está sujeita a vícios de consentimento e possui algum grau de controle sobre a situação de risco, mesmo que limitado; b) a vítima deve ser um indivíduo adulto, capaz e competente para avaliar a extensão do risco envolvido em suas ações; e c) não deve haver a presença de terceiros em uma posição de responsabilidade especial em relação à pessoa que se expôs ao risco.¹²⁶ Exploreemos essas considerações em maior detalhe:

4.4.3. A internet como um Ambiente de Riscos

Em primeiro lugar, é de rememorar que a Internet, como a rede mundial de computadores, é inerentemente um ambiente com riscos. Isso ocorre devido à anonimidade dos contatos, à constante circulação de ameaças por meio de códigos maliciosos e a outras vulnerabilidades.

¹²⁵ SYDOW, Spencer Toth. **Delitos informáticos próprios**: uma abordagem sob a perspectiva vitimodogmática. Orientador: Sergio Salomão Shecaira. 2009. Dissertação (Mestrado no curso de Direito) - Universidade de São Paulo, São Paulo, 2009. p.221

¹²⁶ SYDOW, Spencer Toth. **Delitos informáticos próprios**: uma abordagem sob a perspectiva vitimodogmática. Orientador: Sergio Salomão Shecaira. 2009. Dissertação (Mestrado no curso de Direito) - Universidade de São Paulo, São Paulo, 2009.

Portanto, é de sabença geral a existência de mecanismos de proteção mínimos que os usuários devem adotar para uma navegação segura. Esses mecanismos incluem a utilização de programas de segurança, antivírus, *antispywares*, *antiadwares*, firewalls e a criação de senhas fortes. A não adoção dessas medidas mínimas expõe os usuários a riscos e ameaças, o que pode resultar em violações de dados e outros danos.

A disseminação de informações pela mídia e os alertas constantes dos sistemas operacionais faz com que certas medidas de segurança sejam de conhecimento geral para qualquer usuário interessado em navegar na sociedade informacional. Verdade seja dita, a inclusão digital traz consigo o dever de conscientização sobre a autoproteção contra as ameaças frequentes no ambiente digital. Por outro lado, o letramento digital é uma competência em que a responsabilidade pela segurança recai, em grande parte, sobre o usuário individual. Os usuários têm a liberdade de escolher as medidas de segurança que desejam adotar e os comportamentos que desejam seguir ao usar dispositivos e navegar na internet.

A negligência de um usuário ao não adotar as medidas básicas de proteção, como a instalação de atualizações de segurança, a manutenção do banco de dados de programas maliciosos atualizado (hoje em dia feito pelas próprias aplicações, automaticamente), ou mesmo ao baixar arquivos de origem desconhecida e abrir anexos de e-mails de remetentes desconhecidos, o coloca em uma posição de exposição a riscos. Isso não apenas aumenta as possibilidades de violações de segurança, mas também resulta na falta de proteção adequada para seu patrimônio digital.

De sorte que a decisão do usuário em desobedecer às recomendações de segurança dos dispositivos, guardadas as devidas proporções de assimetria informacional, é uma escolha pessoal, semelhante à decisão de um pedestre atravessar a rua fora da faixa de pedestres. Em ambos os casos, o indivíduo está ciente dos riscos envolvidos, mas opta por seguir adiante por sua própria vontade. A diferença fundamental reside no fato de que, ao atravessar a rua, o pedestre pode visualizar os carros que se aproximam e, com suas ações, talvez consiga evitar um acidente iminente. No entanto, no contexto da rede mundial de computadores, as ameaças e ataques frequentemente ocorrem de forma disfarçada ou imperceptível. Isso resulta em uma

exposição maior aos riscos informáticos quando a vítima negligenciar seu dever objetivo de cuidar da administração e gerenciamento de seus dispositivos.¹²⁷

4.4.4. A ausência de indução por parte de terceiros na criação ou aumento dos riscos

Esse princípio implica que o usuário deve agir de forma desidiosa quanto aos cuidados com seus dispositivos de maneira consciente e livre, sem ser influenciado por terceiros. Ou seja, para que a autocolocação da vítima em risco seja válida, é essencial que não haja influências externas que forcem ou coajam o usuário a adotar práticas inseguras. Isso significa que terceiros não devem manipular, enganar ou persuadir o usuário a agir de forma contrária à sua própria vontade em relação à segurança digital, porquanto, neste caso, estaríamos diante do instituto da heterocolocação em risco.

Em suma, esta premissa pressupõe a independência, a consciência, a liberdade de escolha e a exclusão de influências externas na tomada de decisão do usuário em relação à segurança informática. Para que essa figura seja aplicável, é necessário que o usuário aja de forma desidiosa, consciente e livre, sem ser induzido por terceiros a expor-se a riscos desnecessários. Mesmo porque, se a situação de risco for causada por um terceiro, esse terceiro assume a responsabilidade mínima de garantir a segurança. Portanto, se alguém cria o risco em nome da vítima, não se pode responsabilizar a vítima pela criação da vulnerabilidade, e a situação não se encaixa nesse contexto específico.

4.4.5. A consciência da extensão de riscos

É importante notar que o conhecimento na área da informática está em constante evolução, com conceitos e paradigmas sendo periodicamente atualizados. Isso impõe ao usuário a responsabilidade de manter-se constantemente atualizado. Se a própria vítima assume a responsabilidade de educar-se sobre suas obrigações de segurança e essas informações são amplamente acessíveis ao público, a conduta de terceiros torna-se irrelevante, caracterizando a autocolocação em risco.

¹²⁷ SYDOW, Spencer Toth. **Delitos informáticos próprios**: uma abordagem sob a perspectiva vitimodogmática. Orientador: Sergio Salomão Shecaira. 2009. Dissertação (Mestrado no curso de Direito) - Universidade de São Paulo, São Paulo, 2009. p.222.

Vivemos em uma sociedade de exposição de dados alimentada pelo extenso compartilhamento de informações pessoais em redes sociais, incluindo detalhes como nome, e-mail, imagem, data de nascimento e local de trabalho. Quando esses dados pessoais são tornados públicos dessa forma, isso pode afetar a maneira como o dano alegado pelo titular dessas informações é avaliado.¹²⁸

Se um titular argumenta que sofreu danos devido à divulgação de dados pessoais que ele mesmo escolheu tornar públicos, a responsabilidade de provar que esses danos realmente resultaram do tratamento realizado por terceiros recai sobre o próprio titular (é necessário comprovar o elemento essencial de seu direito).

Transpondo essa ideia do dever de precaução em informática para o âmbito prático, tem-se observado um aumento significativo de ações judiciais movidas por "influenciadores digitais" ou empresários e profissionais autônomos que têm as redes sociais como fonte de renda. Essas ações são resultado de invasões fraudulentas em suas contas por criminosos que se fazem passar por eles. As demandas têm como objetivo atribuir a responsabilidade pelos danos sofridos tanto às operadoras de telefonia (quando a invasão envolve a transferência indevida de números ou a clonagem de chips) quanto às próprias plataformas de mídia social, alegando falhas no dever de segurança e prevenção.

Atualmente, o foco principal tem sido a invasão desses perfis por criminosos que executam o chamado "Golpe da Tabela Pix". Nesse esquema fraudulento, os golpistas assumem o controle dessas contas e divulgam anúncios falsos de investimento, nos quais prometem que os seguidores da conta invadida receberão montantes que variam do dobro ao quádruplo, e até mesmo cem vezes o valor depositado, caso efetuem uma transferência via PIX. Os alvos preferenciais são os perfis que possuem um expressivo número de seguidores e desfrutam de reputação sólida, como é o caso de influenciadores digitais, médicos e profissionais de destaque em suas respectivas áreas.

A estratégia por trás do uso de perfis *hackeados* é utilizar do descuido do titular da conta em não habilitar os mecanismos de autenticação de 2 fatores por aplicativo (2FA), apropriando-

¹²⁸ A própria Lei Geral de Proteção de Dados (LGPD), dentro do contexto analisado, não requer explicitamente o consentimento previsto no artigo 7º, inciso I, quando se trata de dados tornados manifestamente públicos pelo próprio titular, conforme estipulado no §4º do mesmo dispositivo legal. Isso ocorre porque os dados que foram tornados públicos pelo próprio titular podem ser tratados de maneira análoga ao instituto da renúncia. No entanto, é importante ressaltar que mesmo nesses casos em que os dados são públicos por opção do titular, é necessário que se respeitem os direitos do titular e os princípios estabelecidos na lei sob pena de estar-se diante da ocorrência de abuso de direito.

se da conta e modificando as credenciais de acesso de modo a impossibilitar ao usuário que retome seu acesso à conta sem acionar a plataforma. Para conferir maior credibilidade ao "anúncio" de "investimento", os criminosos costumam invadir justamente estas contas de *influencers* induzindo as vítimas a acreditarem que estão lidando com uma pessoa conhecida e de confiança.

Ou seja, geralmente o fraudador, que já tinha acesso prévio aos dados da primeira vítima (a proprietária do perfil visado nas redes sociais), aproveita-se de descuidos desta última no que diz respeito ao fornecimento e gerenciamento de senhas, bem como na não adoção de mecanismos mínimos de segurança, ou na participação em campanhas, cliques em links e acesso a sites maliciosos (*phishing*). A partir desse ponto, os cibercriminosos podem roubar dados pessoais, controlar perfis em redes sociais e/ou instalar malware com o mesmo propósito, concretizando a fraude.

Com efeito, estas pessoas só se tornam "vítimas" de supostos fraudadores porque, mesmo dependendo das redes sociais para obter renda, não tomaram as medidas necessárias para gerenciar as configurações da plataforma, incluindo as opções de acesso, segurança e privacidade. Se essas pessoas tivessem habilitado a autenticação de dois fatores por aplicativo teriam evitado, em qualquer cenário, a invasão de suas contas no Instagram e em outras aplicações, mesmo no caso de clonagem.

Mesmo que inicialmente fosse compreensível que as pessoas tivessem certo desconhecimento sobre as táticas dos cibercriminosos nos primeiros casos de invasões em plataformas como Instagram e Facebook, quando esses métodos eram novos e desconhecidos, atualmente não parece encontrar tanto respaldo jurídico que os usuários, especialmente os profissionais que dependem das redes sociais para autopromoção ou como fonte de renda, continuem a tentar atribuir a responsabilidade por suas próprias ações, como a falta de uso de recursos de segurança de acesso, unicamente às empresas.

No Tribunal de Justiça do Estado do Rio de Janeiro, o Juiz José Guilherme Vasi Werner compartilhou da mesma conclusão ao analisar um caso judicial envolvendo concessionária de telefonia. A ação em questão era uma ação de indenização movida contra a operadora Vivo por um autor que alegava que, devido à clonagem de seu chip, indivíduos mal-intencionados conseguiram acessar seus e-mails e criptoativos mantidos em diferentes carteiras eletrônicas.

O juiz argumentou que as ações atribuídas à empresa ré, como um atendimento inadequado que resultou no sim swap, não estariam diretamente ligadas à subtração das criptomoedas em uma "cadeia causal":

“Ainda que se admitisse como verdadeira a narrativa apresentada pelo Autor, os danos sofridos pela suposta falha na prestação do serviço se encontram distantes da conduta praticada pela Ré dentro da cadeia causal. Entender que a falha na prestação do serviço acarretaria a responsabilização da Ré por todo e qualquer dano sofrido de forma subsequente seria transformar a Ré em responsável solidária universal, independentemente da distância do dano dentro da cadeia de causalidade.

Em outras palavras, permitir-se-ia que a falha na prestação do serviço fosse tida como causa para fatos futuros, adotando o regresso *ad infinitum* para responsabilizar a Ré

Assim, é imprescindível que o consumidor, vítima dos danos, demonstre satisfatoriamente que a falha na prestação do serviço tenha sido causa direta e imediata do dano sofrido, ou seja, que as fraudes perpetradas contra os demais serviços prestados por sociedades empresárias diversas tenham tido como causa a falha da prestação do serviço, na origem.

Ou seja, é fundamental que o Autor prove, ainda que minimamente, que a supressão patrimonial tenha sido causada, de forma inequívoca, pelo golpe SIM SWAP, traçando um caminho claro de causalidade entre a conduta (falha no dever de segurança da titularidade da linha telefônica) e o dano (fraude em serviços diversos).

Todavia, o Autor não produz as referidas provas, adotando conjecturas no sentido de afirmar que houve vazamento de dados pessoais pela Ré, o que teria permitido que terceiro acessasse as contas digitais do Autor” (Processo 0805606-23.2023.8.19.0209)

A decisão judicial reflete a preocupação do magistrado em analisar a participação de cada parte no evento deflagrado afastando a aplicação de possível "solidariedade universal" à operadora de telefonia, que no caso daqueles autos seria responsável tanto pelos riscos assumidos pelos usuários na condução de sua atividade profissional (*influencers digitais*), quanto por eventuais falhas de segurança relacionadas a aplicativos de internet gerenciados por terceiros.

Por óbvio, não se está defendendo, ao expor a figura da autocolocação da vítima em risco, que a vítima tem intenção de ter seu direito lesado. Em verdade, apesar da geração do risco, a vítima acredita que o desfecho quanto a seus direitos não será a ela prejudicial.

Também, não se está defendendo a ideia de que a atitude da vítima justifica a conduta do vitimário e o exime de ser punido pelos atos de prejuízo que cometeu em qualquer caso. O que se quer, ao tratar deste instituto, é reduzir o estudo às hipóteses de modulação da reprovabilidade da atitude do autor nos crimes informáticos, pois que, se houve contribuição da vítima lesada quanto a seu bem particular (bem este que poderia ser espontaneamente lesado, destruído, alienado, etc), tal ação deve ter repercussão jurídica.

4.6. A MÁ GESTÃO DE SEGURANÇA DA IDENTIDADE DIGITAL PELO TITULAR, OU DOS MECANISMOS QUE DISPUNHA PARA PROTEGÊ-LA, COMO EXCLUDENTE (INTEGRAL OU PARCIAL) DE RESPONSABILIDADE CIVIL DO AGENTE DE TRATAMENTO, PROVEDOR OU FORNECEDOR EM CUJO SISTEMA O CRIMINOSO SE PASSOU POR ELE.

Como destacado ao longo desta pesquisa, o Código Civil não prevê um rol específico de excludentes de causalidade ou do nexo causal, mas apenas faz menções esparsas no decorrer do texto legal sobre tais hipóteses que, via de regra, exoneram o agente do dever de indenizar.

O caso fortuito e a força maior são eventos que não podem ser evitados devido à sua imprevisibilidade ou irresistibilidade, o que geralmente os torna causas excludentes de responsabilidade civil. Segundo a doutrina, esses são eventos externos às ações do agente, caracterizados por serem inevitáveis e são considerados a causa principal do dano. Portanto, podemos identificar duas características principais desses eventos: sua natureza externa e sua inevitabilidade.

O Código Civil brasileiro estabelece a culpa da vítima como uma das causas excludentes de responsabilidade civil. Isso significa que, em certas situações, se a vítima agir de forma negligente ou contribuir para a ocorrência do dano de maneira significativa, sua própria conduta pode ser considerada como um fator que exclui a responsabilidade do agente causador do dano. Essa previsão pode ser encontrada nos artigos 625, inciso I; 936; e 945 do Código Civil.

No entanto, a doutrina jurídica aponta para uma distinção importante entre o uso do termo "culpa da vítima" e a causa real da exclusão da responsabilidade. De acordo com essa análise, as causas excludentes estão mais relacionadas ao pressuposto do nexo causal do que à culpa da vítima em si. O correto, de acordo com essa visão, seria utilizar o termo "fato exclusivo da vítima".

A razão para essa distinção está na importância de estabelecer a relação de causalidade entre a conduta da vítima e o dano. Em outras palavras, a análise não se limita apenas à avaliação da culpa moral da vítima, mas sim se o comportamento dela teve um papel relevante e direto na ocorrência do dano. Portanto, o foco é determinar se a conduta da vítima desencadeou o evento danoso de forma substancial.

Assim, o termo "fato exclusivo da vítima" enfatiza que a ação ou omissão da própria vítima desempenha um papel fundamental na exclusão da responsabilidade civil, não apenas a

culpa moral. Isso permite uma análise mais precisa da relação de causalidade entre a conduta da vítima e o dano, que é o cerne da questão quando se trata de causas excludentes de responsabilidade civil.

É relevante observar que a causa que exclui a responsabilidade civil devido ao fato exclusivo da vítima, ao quebrar o vínculo causal, é aplicável inclusive em situações abrangidas pela responsabilidade objetiva. Essa interpretação foi esclarecida no Enunciado 459, emitido pelo Conselho de Justiça Federal durante a V Jornada de Direito Civil. Este enunciado estabeleceu o seguinte entendimento: “A conduta da vítima pode ser fator atenuante do nexo de causalidade na responsabilidade civil objetiva”.¹²⁹

O último inciso do artigo 43 da Lei Geral de Proteção de Dados (LGPD), em consonância com o macrossistema do Código Civil, reproduz esta causa de exclusão de responsabilidade.

A título de exemplo de situações que poderiam atrair a hipótese em tela, é possível mencionar:

- (i) Exposição de dados pessoais pelo próprio titular em redes sociais: Quando o próprio titular compartilha informações pessoais em plataformas de redes sociais e, por descuido ou negligência, expõe dados que possam violar sua privacidade e intimidade, a responsabilidade do controlador de dados pode ser excluída. Isso ocorre porque a causa direta do dano é a ação do próprio titular ao compartilhar essas informações.
- (ii) Divulgação voluntária de informações pessoais: Quando o titular dos dados divulga voluntariamente informações pessoais, como uma gravidez, imagens, notícia de uma doença, ou outras informações semelhantes, sem tomar as devidas precauções para ocultar dados que possam afetar sua privacidade, a responsabilidade do controlador de dados não se configura. O dano é decorrente da escolha do titular de compartilhar essas informações.
- (iii) Compartilhamento de senha de acesso: Se o próprio titular compartilha sua senha de acesso ao sistema do agente de tratamento de dados, e o dano resultante desse compartilhamento é exclusivamente causado pelo acesso não autorizado de terceiros, a responsabilidade do controlador pode ser excluída. A senha é uma forma de autenticação, e compartilhá-la implica um risco conhecido pelo titular.

¹²⁹ Disponível em: <https://www.cjf.jus.br/enunciados/enunciado/413>. Acesso em: 21 nov. 23

Ademais, como mencionado no tópico de “consequências da atitude da vítima”, a questão da culpa concorrente, ou fato concorrente, no contexto de delitos como a fraude de identidade, desempenha um papel relevante na análise da responsabilidade civil. A culpa concorrente não exclui a responsabilidade civil, mas sim atua como um elemento de atenuação, levando em consideração a proporção das contribuições das partes para o evento danoso. Aqui, é fundamental destacar a diferença entre a culpa concorrente e a exclusão de responsabilidade, uma vez que a primeira não elimina a responsabilidade, mas a reduz com base na análise do comportamento das partes envolvidas.

No contexto da responsabilidade civil, o Código Civil prevê a culpa concorrente em alguns casos específicos. Por exemplo, o parágrafo único do artigo 738 permite que o juiz reduza equitativamente a indenização devida à vítima em casos de transporte, se esta transgrediu normas e instruções regulamentares estabelecidas pelo transportador. Da mesma forma, o artigo 945 do Código Civil estipula que a indenização será fixada com base no comportamento da vítima em confronto com o do autor do dano, nos casos em que a vítima tenha contribuído para o evento danoso.

Nesse panorama, o fato concorrente atua como um guia para a determinação do valor da indenização. O juiz é encarregado de avaliar a proporção de responsabilidade pelo dano entre a conduta da vítima e do autor do dano, levando em consideração as causas concorrentes. Isso significa que a quantia a ser indenizada será calculada com base na análise equitativa das contribuições de ambas as partes para o evento danoso.

No caso da fraude de identidade, a culpa concorrente poderia ser aplicada se o titular dos dados, de alguma forma, contribuiu para a ocorrência do evento danoso. Por exemplo, se o titular compartilhou sua senha de acesso ao sistema ou negligenciou medidas básicas de segurança, isso poderia ser considerado um fato concorrente que atenuaria a responsabilidade do agente de tratamento de dados.

No Enunciado 630, do Conselho de Justiça Federal, na VIII Jornada de Direito Civil, foi firmado o seguinte entendimento:

Culpas não se compensam. Para os efeitos do art. 945 do Código Civil, cabe observar os seguintes critérios: (i) há diminuição do quantum da reparação do dano causado quando, ao lado da conduta do lesante, verifica-se ação ou omissão do próprio lesado da qual resulta o dano, ou o seu agravamento, desde que (ii) reportadas ambas as condutas a um mesmo fato, ou ao mesmo fundamento de imputação, conquanto

*possam ser simultâneas ou sucessivas, devendo-se considerar o percentual causal do agir de cada um.*¹³⁰

Por fim e não menos importante, vale destacar que em certas situações o ordenamento jurídico estabelece a responsabilidade por atos de terceiros, de modo que o dever de indenizar não é afastado. Isso pode ocorrer por diversas razões, incluindo o fato de que o terceiro faz parte do risco inerente à atividade, o que se relaciona ao conceito de fortuito interno discutido anteriormente. Além disso, a legislação pode impor a obrigação legal de responsabilidade pelo ato de terceiros em determinadas circunstâncias.

Um exemplo claro disso é encontrado no artigo 932 do Código Civil brasileiro, que estabelece diversas situações em que terceiros podem ser responsabilizados por atos de outras pessoas. Por exemplo, os pais podem ser responsáveis pelos atos de seus filhos menores, os empregadores podem ser responsáveis pelos atos de seus empregados no exercício de suas funções, e assim por diante. Essas regras refletem a ideia de que, em certos contextos, é justo e necessário impor a responsabilidade de terceiros pelos atos daqueles sobre os quais têm controle ou cuja conduta está relacionada à atividade que estão realizando. Essas disposições legais demonstram como o ordenamento jurídico pode estabelecer a responsabilidade por atos de terceiros em situações específicas para garantir a proteção dos direitos das partes afetadas.

5. CONCLUSÃO

Nos últimos anos, o mundo passou por transformações drásticas devido à revolução digital, especialmente a partir da popularização da Internet e de mecanismos tecnológicos automatizados que dependem dela ou com ela interagem. Essas mudanças geraram novos padrões culturais e estilos de vida, introduzindo novos conceitos e perspectivas sobre ideias já estabelecidas. A noção de identidade, que tem raízes antigas, agora se apresenta de maneira diferente. A ciberidentidade emergiu como um componente integral da identidade, composta por todos os dados pessoais relacionados a uma pessoa real, identificável ou identificada. A proteção desses dados tornou-se fundamental, considerando a dignidade da pessoa humana e a constituição de um direito fundamental à privacidade.

¹³⁰ Disponível em: <https://www.cjf.jus.br/enunciados/enunciado/1204>. Acesso em: 22 set. 23

Com a ampliação do conceito jurídico de identidade, surgiram novas ameaças. O ciberespaço, como principal ambiente para o armazenamento e a transferência de informações, é amplamente explorado por entidades governamentais, empresas e criminosos para acessar dados pessoais e informações em geral. Era inevitável o surgimento do fenômeno da usurpação de identidade e seu conseqüente crescimento, em escala e gravidade, à medida que a tecnologia avançou e a prestação de serviços e interação humanas se transferiram massivamente para o mundo virtual.

Este fenômeno não é exclusivo do Brasil, mas é global. Como consequência, as mudanças trazidas pela tecnologia têm um impacto significativo na forma como o Direito precisa se adaptar e interpretar seus princípios e valores para lidar com os desafios crescentes relacionados à proteção da identidade pessoal na era da informação, tanto em face dos indivíduos quanto das organizações que comportam estas tecnologias.

Essas são as circunstâncias que levam à conclusão de que o bem jurídico mais precioso a ser tutelado na Era Digital é a informação. No entanto, a falta de padrões internacionais para combater crimes cibernéticos torna os esforços de proteção cibernética muitas vezes ineficazes. Os recursos públicos são limitados em comparação com os recursos dos criminosos, e a legislação (e sua aplicação) por vezes fica para trás em relação à evolução tecnológica.

Ficou claro ao longo desta pesquisa que os usuários da Internet muitas vezes - com efeito, frequentemente e primariamente - desempenham papel importante em sua própria segurança cibernética. Justamente por isso, é crucial que compreendam não apenas como usar, mas de que modo funciona o ambiente em que estão navegando. Só assim, estarão cientes das ameaças e despertarão para a necessidade de se protegerem o que, espera-se, os levará à busca por letramento digital (autonomamente)¹³¹. A vitimodogmática, que estuda o comportamento da vítima na gênese do delito, enfatiza a ideia de que os cidadãos têm responsabilidade na prevenção da vitimização, sendo corresponsáveis por suas ações ou omissões na prevenção de crimes.

Embora existam ferramentas como firewalls e antivírus, sua eficácia depende de como os usuários as utilizam. A simples confiança na tecnologia não é suficiente para garantir a

¹³¹ Não se desconhece o debate sobre letramento digital como parte da educação básica, mas não é objetivo deste trabalho examinar a questão que está fora de seu recorte. Deste modo, foca-se apenas na possibilidade e na importância de que esta seja uma escolha pessoal dos usuários em decorrência da compreensão da insegurança online, como é, intuitivamente, a adoção de cuidados nos espaços públicos e regiões perigosas do mundo físico ou extravirtual.

segurança online; cada usuário deve considerar-se um administrador de seus próprios ativos jurídicos virtuais e tomar medidas proativas para protegê-los.

Ao examinar-se a responsabilização por danos decorrentes da apropriação indevida da identidade pessoal digital, constatou-se que seria viável dentro do atual sistema legal, bastando para isso a ressignificação de conceitos e um ajuste no raciocínio (*mindset*) dos aplicadores do direito.

Isso é constatado após uma análise do Direito Civil sob a perspectiva solidarista, com foco na proteção da pessoa humana, conforme estabelecido nos imperativos constitucionais. No entanto, é evidente que existe uma lacuna na aplicação eficaz das causas excludentes de ilicitude pelo judiciário, além da necessidade de reconhecer que parte dos delitos é facilitada pelo próprio ofendido devido à falta de precaução.

Em primeiro lugar, é importante observar que uma abordagem Civil-Constitucional exige uma visão abrangente do ordenamento jurídico, considerando-o como um todo, com a Constituição como guia principal. Isso implica que o exercício de direitos e garantias fundamentais não depende exclusivamente da legislação infraconstitucional, mas também da interpretação dos princípios e valores emanados do texto constitucional para sua concretização.

Essa análise tem um impacto significativo na responsabilidade civil, reconhecendo as desigualdades de poder na sociedade e enfatizando a responsabilidade coletiva de proteger os vulneráveis em prol do bem comum, uma responsabilidade que, na verdade, recai sobre todos os indivíduos. Isso estabelece um ideal solidarista comprometido com a proteção das vítimas de danos e com a criação de um ambiente social mais seguro para todos.

No entanto, a responsabilidade civil, que envolve o dever de não prejudicar os outros, não se limita à sua dimensão reparadora. Para a proteção eficaz dos direitos fundamentais, é necessário um esforço coletivo para evitar danos e mitigar os riscos das atividades. Para tanto, é crucial tomar decisões coletivas e informadas sobre os riscos que as pessoas estão dispostas a tolerar enquanto sociedade, considerada a pluralidade de percepções.

A atividade de tratamento de dados pessoais, embora possa apresentar riscos, oferece inúmeros benefícios não apenas para os indivíduos, mas também para a sociedade e a economia como um todo. Tanto é verdade, que a Lei Geral de Proteção de Dados (LGPD) reconhece não apenas os direitos pessoais, como privacidade e liberdade de expressão, mas também considera o desenvolvimento econômico, tecnológico e a inovação como fundamentos importantes.

Os direitos individuais relacionados à Internet são protegidos por uma série de normas, desde a Constituição Federal até leis específicas, como o Marco Civil da Internet e a LGPD de sorte que, nos últimos anos, houve um considerável desenvolvimento da legislação relacionada à Internet e à tecnologia. Contudo, a doutrina de reparação civil para vítimas de ilícitos nessa área ainda carece de atenção especial pelo Judiciário sobretudo em razão de suas peculiaridades, como o anonimato do ofensor, rápida disseminação de conteúdo, dificuldade na remoção de conteúdo ilícito, dano permanente e continuado, tratamento do mesmo tipo de dados pessoais por diversos agentes com consequente dificuldade de identificação do verdadeiro responsável por conduta reputada como ilícita, entre outros.

Logo, e em segundo lugar, percebe-se que o instituto da responsabilidade civil desempenha um papel fundamental não apenas na garantia da reparação efetiva de danos, mas também na promoção de ações relacionadas à educação digital, aumento da segurança da informação, resolução de conflitos de direitos e orientação da atividade judicial para assegurar a completa reparação das vítimas, sem banalizar o instituto. Isso contribui para um ambiente digital mais seguro e responsável.

As excludentes de responsabilidade, a seu turno, servem à compreensão dos limites da responsabilidade civil, particularmente em um contexto marcado pela crescente importância da proteção de dados pessoais. No entanto, frequentemente a disciplina das excludentes é negligenciada em favor da ênfase na qualidade reparatória.

Nesse contexto, a doutrina e a jurisprudência possuem grande relevância na discussão de questões relevantes relacionadas às excludentes de responsabilidade civil e na sistematização desse instituto, especialmente quando as leis especiais não abordam o assunto de maneira satisfatória ou quando a interpretação das leis existentes é complexa.

As excludentes aqui defendidas têm o propósito de eliminar os pressupostos sem os quais não há responsabilidade civil. Estes pressupostos incluem a ilicitude do ato lesivo e a existência de nexo causal. Esses requisitos são refletidos tanto nas excludentes gerais quanto nas especiais previstas no artigo 43 da LGPD, pois: (i) Se os agentes de tratamento de dados não realizaram o tratamento de dados pessoais atribuído a eles, falta o pressuposto do nexo causal; (ii) Se não houve violação da legislação de proteção de dados, não há ato ilícito e (iii) Se a culpa exclusiva for do titular dos dados ou de terceiros, o nexo causal também é afastado.

Nesse ínterim, notório que as excludentes desempenham um papel crucial no ideário de Justiça, não apenas por constituírem meios de defesa essenciais, especialmente em um cenário

onde a responsabilidade tende a ser objetiva, mas também por representarem princípios universais que buscam estabelecer o equilíbrio necessário entre responsabilidade e irresponsabilidade. Esse equilíbrio visa evitar injustiças decorrentes da responsabilização de terceiros que não deveriam ser responsáveis pelo dano causado.

Estabelecer um fio condutor que permita a sistematização do instituto das excludentes é uma tarefa desafiadora para os intérpretes, uma vez que a legislação muitas vezes trata dessa questão de forma precária. A doutrina e a jurisprudência desempenham um papel vital na evolução do entendimento das excludentes, mas ainda há muito trabalho a ser feito nesse aspecto.

À guisa de conclusão, realmente, confirmaram-se as hipóteses de que (i) o pleno gozo do direito à dignidade passa pela tutela da ciberidentidade que não se confunde com a proteção de dados pessoais; (ii) uma das principais ameaças a este direito decorre da sofisticação, reiteração e consequências sócio-financeiras das fraudes; (iii) a usurpação de identidade é um processo de duas etapas nas quais será impossível pensar em eficácia legislativa ou de tutela judicial sem a conscientização dos titulares da ciberidentidade; e (iv) a má gestão de segurança de sua identidade digital, quando providos os mecanismos e as informações para agir de modo diverso, podem constituir excludente de responsabilidade de agentes de tratamento, provedores e fornecedores.

Ou seja, limitando-se a análise ao ambiente das fraudes de identidade na esfera do direito privado, em um modelo híbrido de sociedade física-virtual, a tutela da ciberidentidade só será viável e realizável quando despendidos esforços concomitantes e autônomos do Poder Público, da iniciativa privada e dos titulares de identidades, atribuindo-se igual importância às três contribuições.

Caso o titular insista em se manter como o “elo fraco” da corrente, deverá arcar com o custo jurídico e pessoal da sua escolha, eximindo proporcionalmente os provedores, fornecedores ou agentes de tratamento da responsabilidade civil (accountability), na medida em que o ato ilícito (praticado no “espaço” destas plataformas ou serviços”) tenha ocorrido por culpa exclusiva ou concorrente da vítima.

REFERÊNCIAS

ALVES, Marco Antônio; DINIZ, Thiago Dias de Matos; CASTRO, Viviane Vidigal de. **Criminologia e cybercrimes**. Belo Horizonte: RECAJ – UFMG, 2020. 13 p.

AMARAL, Francisco. **Direito Civil**: introdução. 10. ed. revista e modificada. São Paulo: Saraiva Educação, 2018. 372 p.

ANTOLISEI, Francesco; CONTI, Luigi. **Manuale di diritto penale / [1], Parte generale**. Milano: A. Giuffrè, 2003. 880 p.

ANTUNES, Ricardo. **Desenhando a nova morfologia do trabalho**: As múltiplas formas de degradação do trabalho. Revista Crítica de Ciências Sociais (Coimbra), n.º 83, 2008, 15 p. Disponível em: <https://doi.org/10.4000/rccs.431>. Acesso em 10 set. 2023.

AREOSA João. Do risco ao acidente: Que possibilidades para a prevenção?. Luanda: **Revista Angolana de Sociologia**, n.º 4, 2009. 26 p.

AZEVEDO, Antonio Junqueira de. **Crítica ao personalismo ético da constituição da república e do código civil**. Em favor de uma ética biocêntrica. [s.l.: s.n.], 2008. 12 p.

BEALS, Michaela; DELIEMA, Marguerite; DEEVY, Martha. **Framework for a taxonomy of fraud**. Financial Fraud Research Center, 2015. 40 p.

BECK, Ulrich. **Sociedade de risco mundial**: em busca da segurança perdida. Edições 70, 2015. 423 p.

BECK, Ulrich. **Risk society. Towards a new modernity**. Londres: Sage, 1992. 272 p.

BECK, Ulrich; GIDDENS, Anthony.; LASH, Scott. **Modernização reflexiva: Política, tradição e estética na ordem social moderna**. Oeiras: Celta Editora, 2000. 336 p.

BITTAR, Carlos Alberto. **Reparação Civil por Danos Morais**. 4. ed., rev., aum. e mod. por Eduardo Carlos Bianca Bittar. São Paulo: Saraiva, 2015. 373 p.

BITTAR, Carlos Alberto. **Responsabilidade Civil**. Teoria e Prática. Atualização de Eduardo Carlos Bianca Bittar. 4. ed. Rio de Janeiro: Forense Universitária, 2005. 144 p.

BITTENCOURT, Cezar Roberto. Tratado de Direito Penal – Volume 3, 3ª Edição. São Paulo: Editora Saraiva, 2006. 1096 p.

BOLESINA, Iuri.; GERVASONI, Tamiris Alessandra. **O direito à identidade pessoal no Brasil e seus fundamentos jurídicos na atualidade**. v. 8, n. 13, 23 p.

BRAGA NETTO, Felipe Peixoto; FARIAS, Cristiano Chaves; ROSENVALD, Nelson. **Tratado de Responsabilidade Civil**. 3. ed. São Paulo: Saraiva Educação, 2018. 1480 p.

BRASIL. **Emenda Constitucional nº 155 de 10 de fevereiro de 2022**. 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. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em 15 set 2023.

BRASIL. **Lei nº 12.737**, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm. Acesso em 20 set 2023.

CALLEGARI, André Luís; ANDRADE, Roberta Lofrano. Sociedade do risco e direito penal. **Revista da Defensoria Pública do Estado do Rio Grande do Sul**, Porto Alegre, n. 26, p. 115–140, 2020.

CAMPOS, Ligia Fabris. **O Direito de ser si mesmo**: a tutela da identidade pessoal no ordenamento jurídico brasileiro. Dissertação (Mestrado em direito) - Pontifícia Universidade Católica: Rio de Janeiro, PUC-RJ, 2006. 375 p.

CANCELIER, Mikhail Vieira de Lorenzi. **O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro**. SEQUENCIA, v. 38, p. 213-240, 2017. Disponível em: <<https://www.scielo.br/pdf/seq/n76/2177-7055-seq-76-00213.pdf>>. Acesso em: 22 set. 23.

CARNEIRO DA SILVA, Flávio Manuel. **A usurpação da ciberidentidade**. Dissertação de Mestrado —Universidade Católica Portuguesa. 2004. 57 p.

CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. 15. ed. Barueri: Atlas, 2021. 672 p.

Código Civil Português. **Decreto-Lei nº 47344/66**. Diário da República Eletrônico. Disponível em: <https://dre.pt/web/guest/pesquisa/-/search/477358/details/normal?l=1> – Acesso em: 22 set. 23.

CORDEIRO, Euller Xavier. Vitimodogmática: Uma análise dogmática do comportamento da Vítima *In*: FALEIROS JÚNIOR, Roberto Galvão. (Ed.). **Estudos contemporâneos de vitimologia**. São Paulo: Cultura Acadêmica: Editora UNESP, 2011. 159 p.

Corte IDH. **OC 24/2017**, Parecer consultivo sobre identidade de gênero, igualdade e não discriminação entre casais do mesmo sexo, de 24-11-2017, solicitado pela República de Costa Rica. [Tradução livre]. Disponível em: https://www.corteidh.or.cr/docs/opiniones/seriea_24_por.pdf. Acesso em: 20 nov.2023.

CHOERI, Raul Cleber da Silva. **O direito à identidade na perspectiva civil-constitucional**. Rio de Janeiro: Renovar, 2010. 365 p.

COUTINHO, Marina de Alencar Araripe. **A proteção da vítima de danos causados por uma inteligência artificial: uma perspectiva civil-constitucional**. Orientador: Prof. Dr. Fabiano Hartmann. 2022. Dissertação (Mestrado no curso de Direito) - Universidade de Brasília, Brasília, 2022. 129 p.

DELIEMA, Marguerite; MOTTOLA, Gary; DEEVY, Martha. 2017. Findings from a pilot study to measure financial fraud in the United States. Stanford Center on Longevity Working Paper. February *apud* FONSECA, Ana Catarina Cardoso. **Fraude ao consumidor online: variáveis explicativas da vitimação e reportagem**. 2021. 107 p.

DOUGLAS, Maria. e WILDAVSKY, Aaron. **Risk and culture: An essay on the selection of technological and environmental dangers**. Berkeley (CA): University of California Press, 1982. 224 p. Disponível em: <https://www.jstor.org/stable/10.1525/j.ctt7zw3mr>. Acesso em: 20 set. 2023.

EISER, J. Richard. **Public perception of risk**. UK: Report prepared for Foresight, Office of Science and Technology, 2004. 11 p. Disponível em: <https://www.jstor.org/page-scan-delivery/get-page-scan/41376908/0>. Acesso em: 20 set. 2023.

FACHIN, Luiz Edson. Direitos Fundamentais, dignidade da pessoa humana e o novo Código Civil: uma análise crítica. *In*: SARLET, I.W. (org). **Constituição, direitos fundamentais e direito privado**. Porto Alegre: Livraria do Advogado, 2ª ed., 2006. 17 p.

FACCHINI NETO, Eugênio. Reflexões histórico-evolutivas sobre a constitucionalização do direito privado. In: SARLET, **Ingo Wolfgang** (org). **Constituição, direitos fundamentais e direito privado**. Porto Alegre: Livraria do Advogado, 2ª ed., 2006. 49 p.

BRAGA NETTO, Felipe Peixoto; FARIAS, Cristiano Chaves; ROSENVALD, Nelson **Novo Tratado de Responsabilidade Civil**. 4. ed. São Paulo: Saraiva Educação, 2019. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788553612086/>. Acesso em: 21 set. 23.

FONSECA, Ana Catarina Cardoso da. **Fraude ao consumidor online: variáveis explicativas da vitimação e reportagem**, Orientadores: Dra. Inês Guedes e Dr. Samuel Moreira. 2021. Dissertação (Mestrado no curso de Direito) - Universidade de Porto, Portugal, 2021. 162p.

FISCHHOFF, Baruch; WATSON, Stephen R; HOPE, Chris. **Defining risk, Policy Sciences**, 1984, n.º 17, 17 p.

GIDDENS, Anthony. **O mundo na era da globalização**. Lisboa: Editorial Presença, 2000, 48p.

GRECO, Alessandra Orcesi Pedro. **A Autocolocação da Vítima em Risco**. São Paulo: Editora RT, 2004. 192 p.

Goiá Schmaltz, Diego.; MPDFT. **Recurso Extraordinário 363.889/DF**. j. 2 jun. 2011. Disponível em: <<https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=1638003>>. Acesso em: 20 nov. 2023

GOLDSTEIN, Raúl. **Diccionario de derecho penal y criminología**. [s.l: s.n.], 1993, 677 p.

GREEN, Judith. **Risk and misfortune: The social construction of accidents**. Londres: Routledge, 1997. 232 p.

HRYNIEWICZ, Severo; SAUWEN, Regina Fiuza. **O Direito “in vitro” da Bioética ao Biodireito**. 3ª edição. Rio de Janeiro: Lumen Iuris Editora, 2008. 254 p.

JAKOBS, Günther. **A Imputação Objetiva no Direito Penal** (tradução André Luis Callegari), 2ª Edição. Editora Revista dos Tribunais, São Paulo, 2014. 96 p.

KEMP, Steven; MONEVA, Asier. **Fraude online vs. offline: Factores predictores de victimización y su impacto.** InDret, 2020. 20 p.

KÄVRESTAD, Joakim. **Defining, categorizing and defending against online fraud.** University of Skövde, 2014. 81 p.

MATOS, Eneas de Oliveira. **Dano moral e dano estético.** Rio de Janeiro: Renovar, 2008. 365 p.

MELIÁ, Manuel Cancio. **Conducta de la víctima e imputación objetiva en derecho penal : estudio sobre los ámbitos de responsabilidad de víctima y autor en actividades arriesgadas.** Bogotá: Universidad Externado De Colombia, 2001. 675 p.

MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **REI - Revista Estudos Institucionais**, 6(2), pp. 507–533. Disponível em: <https://doi.org/10.21783/rei.v6i2.521>. Acesso em: 21 set. 23.

MONTEIRO FILHO, Carlos Edison do Rêgo; ROSENVOLD, Nelson **Danos causados a dados pessoais: novos contornos.** Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/332618/danos-causados-a-dados-pessoais--novos-contornos> - Acesso em: 21 set. 23.

MORAES, Maria Celina Bodin de. Risco, solidariedade e responsabilidade objetiva. **Revista dos Tribunais**, v. 854, 2006. 26 p.

MOREIRA FILHO, Guaracy. **Vitimologia – O papel da Víctima na Gênese do Delito.** São Paulo: Editora Jurídica Brasileira, 2004. 187 p.

MORSELLO, Marco Fábio. **Contrato de Transporte: novos paradigmas do caso fortuito e força maior.** São Paulo: Thomson Reuters Brasil, 2021. 424 p.

MULHOLLAND, Caitlin Sampaio. **A responsabilidade civil por presunção de causalidade.** Rio de Janeiro: GZ Editora, 2010. 366 p.

OLIVEIRA, Bruna Machado de. *et al.* Crimes virtuais e a legislação brasileira. **(Re) Pensando o Direito. Rev. Do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo.** v. 7, n. 13, 2017. 13 p.

PEREIRA, Caio Mário da Silva. **Responsabilidade civil**. 10. ed. Rio de Janeiro: GZ, 2012. 464 p.

PERROW, Charles. **Normal accidents: living with high-risk technologies**. New Jersey: Princeton University Press, 1999. 464 p.

PIERANGELI, José Henrique. **O Consentimento do Ofendido na Teoria do Delito**. 3ª Edição revista e atualizada. São Paulo. Editora Revista dos Tribunais. 2001. 284 p.

PINO, Giorgio. Il diritto all'identità personale ieri e oggi. Informazione, mercato, dati personali. *in*: **Libera circolazione e protezione dei dati personali**. [s.l.] Giuffrè Editore, 2006.

RAMOS, André Luiz Arnt. A responsabilidade civil para além dos esquemas tradicionais: prospecções do dano reparável na contemporaneidade. **Revista Fórum de Direito Civil - RFDC**. Belo Horizonte, ano 4, n. 10, p. 13-33, set./dez., 2015.

REIS, Eva da Silva Rodrigues Pinto dos. **Apropriação Indevida de identidade: enquadramento jurídico-penal**. Dissertação de Mestrado – Universidade de Lisboa: Faculdade de Direito. 2019. 90 p.

RUZYK, Carlos Eduardo Pianosvki. *et al.* (Org.). **Direito Civil Constitucional: a ressignificação da função dos institutos fundamentais do direito civil contemporâneo e suas consequências**. Florianópolis: Conceito, 2014. 08 p.

SCHREIBER, Anderson. **Novos Paradigmas Da Responsabilidade Civil: da erosão dos filtros da reparação à diluição dos danos**. São Paulo: Editora Atlas, 2ª ed., 2009. 276 p.

SESSAREGO, Carlos Fernandez. **Derecho a la identidad personal**. Buenos Aires: Austrea, 1992. 489 p.

SOARES, Flaviana Rampazzo. **Responsabilidade civil por dano existencial**. [s.l.], 2009. 160p.

STJ. **AREsp nº 2130619 / SP (2022/0152262-2)**; Rel. Francisco Falcão; Órgão Julgador: 2ª Turma do Superior Tribunal de Justiça; j. 07/03/2023.

STOCO, Rui. **Tratado de responsabilidade civil: doutrina e jurisprudência**. São Paulo: Editora Revista Dos Tribunais, 2007. 1949 p.

SYDOW, Spencer Toth. **Delitos informáticos próprios**: uma abordagem sob a perspectiva vitimodogmática. Orientador: Sergio Salomão Shecaira. 2009. Dissertação (Mestrado no curso de Direito) - Universidade de São Paulo, São Paulo, 2009. 282 p.

TEPEDINO, Gustavo. Premissas Metodológicas para a Constitucionalização do Direito Civil. **Revista de Direito do Estado**, ano 1, n. 2, 2006. 16 p.

TEPEDINO, Gustavo. Marchas e contramarchas da constitucionalização do direito civil: a interpretação do direito privado à luz da Constituição da República. **(Syn)Thesis**, v. 5, n. 1, 2012. 06 p.

TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. Inteligência Artificial e Elementos da Responsabilidade Civil. *In*: FRAZÃO, Ana.; MULHOLLAND, Caitlin. (Coord.). **Inteligência Artificial e Direito**: Ética, Regulação e Responsabilidade. 2. ed. São Paulo: Revista dos Tribunais, 2020. 29 p.

TURKLE, Sherry. **Life on the screen: identity in the age of the internet**. London, Weidenfeld & Nicholson, 1996. 352p.

TJSP; **Apelação Cível 1001032-45.2021.8.26.0177**; Rel. Virgílio de Oliveira Junior; Órgão Julgador: 23ª Câmara de Direito Privado; Foro de Embu-Guaçu, Vara Única, j. 01/12/2021; Registro 03/12/2021.

ANEXO

Anexo I – A evolução do “roubo de identidade”

Table 1: Evolution of Identity Theft	
Era	Type of Identity Theft
1800-. 1918	The outlaws of this era killed people to assume their identities
1919- 1921	Identities were stolen to cast votes multiple times
1922- 1930	The smugglers created their own version of witness protection programs and murdered people to attain legal documents to create new identities
1931- 1959	Youngsters created fake IDs to buy alcohol
1960- 1969	Introduction of credit cards gave criminals new ways of identity theft
1970- 1989	Frank Abagnale the famous con artist stole identities to cash cheques
1990- 1998	Technology advancement increased cases of identity crimes
1999- 2000	Introduction of Internet and search engines like Google led people to give away personal information
2001- 2003	The credit reporting agencies were instructed to provide credit reports to customers to prevent fraudulent accounts being opened
2004- 2015	The National Crime Victimization Survey was updated to include new forms of Identity Theft
2016	Identity Theft was the most popular consumer complaint for 15 consecutive years
2017	American banks increased their security causing criminals to use other platforms for stealing identities
2018 - 2020	Technology is evolving and new apps are being introduced; so that thieves are gaining more and more access to personal information through these new apps

Tabela 1: Evolução do Roubo de Identidade (tradução livre)	
Era	Tipo de Roubo de Identidade
1800-. 1918	Os criminosos dessa época matavam pessoas para assumir suas identidades
1919- 1921	Identities eram roubadas para votar várias vezes
1922- 1930	Os contrabandistas criaram suas próprias versões de programas de proteção a testemunhas e assassinavam pessoas para obter documentos legais e criar novas identidades
1931- 1959	Jovens criavam documentos falsos para comprar álcool

1960-1969	A introdução de cartões de crédito deu aos criminosos novas maneiras de roubo de identidade
1970-1989	Frank Abagnale, o famoso golpista, roubou identidades para descontar cheques
1990-1998	O avanço da tecnologia aumentou os casos de crimes de identidade
1999-2000	A introdução da Internet e de mecanismos de busca como o Google levou as pessoas a fornecerem informações pessoais.
2001-2003	As agências de relatórios de crédito foram instruídas a fornecer relatórios de crédito aos clientes para evitar a abertura de contas fraudulentas
2004-2015	O National Crime Victimization Survey foi atualizado para incluir novas formas de roubo de identidade
2016	O roubo de identidade foi a reclamação mais popular dos consumidores por 15 anos consecutivos
2017	Bancos americanos aumentaram sua segurança, levando criminosos a usar outras plataformas para roubar identidades.
2018 - 2020	A tecnologia está evoluindo e novos aplicativos estão sendo introduzidos; assim, os golpistas estão ganhando cada vez mais acesso a informações pessoais por meio desses novos aplicativos

Fonte: IRSHAD, Shareen/ SOOMRO, Tariq Rahim - Identity Theft and Social Media, p.43. ¹³²

¹³²Disponível em: https://www.researchgate.net/profile/Tariq-Soomro-2/publication/323185128_Identity_Theft_and_Social_Media/links/5a850d2aa6fdcc201b9f044c/Identity-Theft-and-Social-Media. Acesso em 25 nov. 2023