# REFLEXÕES JURÍDICAS SOBRE ANONIMATO, LIBERDADE E VULNERABILIDADE DA MULHER NOS APLICATIVOS DE RELACIONAMENTO.

Luciana Duarte Oliveira<sup>1</sup>

**RESUMO:** O artigo propõe uma discussão jurídica acerca da situação de vulnerabilidade das mulheres no uso de aplicativos de relacionamentos. Considerando o funcionamento das plataformas, que pretere a certificação e identificação dos usuários em favor da liberdade dos usuários, estratégia que acarreta a proliferação de perfis falsos, a reflexão cingirá ao anonimato na internet com a consequente responsabilidade das plataformas em prover um ambiente seguro para as usuárias. Fundando-se nos casos relatados, o propósito final do artigo é identificar possíveis medidas que poderiam mitigar os riscos e avaliar tais possibilidades sob a luz dos princípios e garantias jurídicas que regem a legislação Brasileira. Verifica-se, nesse contexto, se a possibilidade de aumentar as exigências de identificação para criação de perfis seria compatível com o ordenamento nacional. Desse modo, será possível concluir acerca da necessidade de ponderação da amplitude da proteção à liberdade para garantir a segurança dos usuários.

**Palavras- Chave**: Aplicativo de Relacionamentos; Anonimato na Internet; Violência contra mulheres.

**ABSTRACT:** The article proposes a legal discussion about the vulnerability of women in the use of relationship apps. Considering the functioning of the platforms, that despises the certification of the identify users in favor of users' freedom, a strategy that leads to the proliferation of fake profiles, the proposed reflection will limit itself to anonymity on the internet with the consequent responsibility of the platforms in providing a safe environment for women users. Based on the few cases reported and mentioned on the essay, the final purpose is to identify possible measures that could mitigate the risks and, therefore, evaluate such possibilities in the light of the legal principles and guarantees that conduct the Brazilian legislation. It is verified, in this context, if the possibility of increasing the identification requirements for the creation of profiles would be compatible with the Brazil's legal order. Thereby, it will be able to draw the conclusion about the need to weigh the extent of the protection to freedom in order to guarantee the safety of the users.

**Keywords**: Dating Apps; Anonymity on the internet; Violence against women.

## INTRODUÇÃO

No início da década de 1990, a aclamada revista New Yorker publicou uma charge para representar o anonimato na internet, característica fundante do incipiente mundo virtual.

<sup>&</sup>lt;sup>1</sup> Mestra em Direito nas Relações Econômicas e Sociais pela Faculdade de Direito Milton Campos. E-mail: <a href="mailto:luduarteo@hotmail.com">luduarteo@hotmail.com</a>

Naquele momento, a rede apenas nascia para o grande público, mas a sátira resume com perfeição as primeiras impressões do fenômeno: dois cachorros conversam defronte a uma tela de um computador; acompanha a imagem a célebre legenda, "na internet, ninguém sabe que você é um cachorro".<sup>2</sup>

Mais de duas décadas depois de sua publicação, mesmo com a inexorável evolução dos meios tecnológicos, com a internet ainda mais presente no dia-a-dia da sociedade, certificar a identidade real do usuário continua a ser uma tarefa nem sempre simples, pois o anonimato, proclamado na charge, ainda é uma característica essencial do mundo virtual. Tome-se o exemplo, as redes sociais, como *Facebook*, *Twitter* ou *Instagram*: em razão da praticidade ao acesso, é possível com enorme facilidade cadastrar e montar um perfil com nome fictício, manipular detalhes da sua vida como idade ou profissão ou, mais gravemente, se passar por outra pessoa existente, como um artista ou político – tudo ao alcance de poucos cliques. A questão da falsidade das informações nos perfis é de tal maneira difundida, que foi possível demonstrar que a falsidade é a *regra* na internet, ao passo que os perfis que contenham informações inteiramente verdadeiras são a exceção no mundo digital (DROUIN, 2016)<sup>3</sup>.

Contudo, nem sempre essa ampla possibilidade de anonimato se manifesta de forma inofensiva ou irrelevante. Há alguns anos surgem relatos de mulheres que se depararam com perfis mantidos em aplicativos de namoro, administrados por indivíduos condenados por crimes sexuais, ou com informações falsas, que utilizavam da plataforma para captar novas vítimas e manter a atividade predatória. A manutenção por meio de informações falsas, ou ainda a presença perfis verdadeiros, porém controlados por indivíduos reiteradamente condenados por crimes sexuais, são duas consequências do mesmo problema: a falta de controle dos usuários dessas plataformas. Tratam-se de exemplos de como a liberdade da rede

-

<sup>&</sup>lt;sup>2</sup> No *cartoon* original, Peter Steir escreveu: "On the Internet, nobody knows you're a dog". A charge foi publicada em 1993 e é, desde então, a mais reproduzida da história da revista; conforme reforça o próprio autor, é ainda mais relevante nos tempos atuais. (CAVNA, 2013).

<sup>&</sup>lt;sup>3</sup> Conforme a pesquisa desenvolvida por Michelle Drouin, Daniel Miller, Shaun M.J. Wehle e Elisa Hernandez, a mentira é perpetuada especialmente em decorrência da forte prevalência da presunção de que os outros estejam mentindo, o que modifica o comportamento do usuário, que opta por manipular suas informações também. Ou seja, os usuários são incentivados a falsearem as informações por estarem certos de que os outros também estão falseando. (DROUIN, 2016).

resulta em um problema na vida física e pode alcançar a esfera jurídica e criminal ao afetar uma área particularmente sensível e perpetuando a exploração da vulnerabilidade da mulher.

A multiplicação de sites e aplicativos que permitem a conexão de indivíduos na busca por "encontrar um par" (como OkCupid, Tinder, Plenty of Fish, Match.com, Grindr, dentre diversos outros) é uma das características dessa internet participativa e democrática que prospera no século XXI. A maioria desses sites de relacionamentos segue uma lógica similar das redes sociais: o usuário interessado monta seu perfil com foto(s), idade, localização, além de informações pessoais como os interesses e *hobbies* para que outros usuários encontrem características em comum. Porém, não demorou a facilidade a esse acesso ser notada pelos agressores e criminosos para propulsionar a infeliz intenção de usar tais plataformas para facilitar a execução de crimes vitimando as mulheres que usam tais plataformas. Ainda assim, apesar de vários casos serem relatados todos os anos, pouca mudança operou no funcionamento desses aplicativos desde o início do fenômeno.

Portanto, dessa situação, pode-se vislumbrar um problema ético, jurídico e social, a ser trabalhado no presente artigo: a dificuldade de garantir, ao mesmo tempo, liberdade e anonimato (ideais calcados na internet desde seus primórdios e reproduzidos nas novéis plataformas), e assegurar o mínimo de segurança para as usuárias dessas plataformas. Com isso, o objetivo do presente artigo é avaliar o panorama jurídico da liberdade e do anonimato na internet, contextualizado ao problema da vulnerabilidade da mulher nos sites e aplicativos de relacionamento. A pesquisa terá caráter bibliográfico e será utilizado o método indutivo4.

## NOÇÕES DE IDENTIDADE E ANONIMATO NA INTERNET

O anonimato propiciado pela internet, principalmente para aqueles que a dominam o suficiente para impô-lo com precisão<sup>5</sup>, produz consequências profundas das mais variadas

<sup>&</sup>lt;sup>4</sup> De acordo com esse método, a pesquisa é conduzida utilizando-se a lógica de "pesquisar e identificar as partes de um fenômeno e colecioná-las de modo a ter uma percepção ou conclusão geral." (PASOLD, 2008, p. 207).

<sup>&</sup>lt;sup>5</sup> Não se pretende aqui discutir as barreiras tecnológicas de uma atuação verdadeiramente anônima da internet. Muitas variáveis podem ser consideradas, dentre elas, a habilidade do usuário de ocultar o IP

naturezas – seja na liberdade de expressão, seja no comércio eletrônico, ou mesmo no aspecto financeiro, no prelúdio da era das *fintechs* e criptoativos<sup>6</sup>. Não é por menos que a vigilância e o anonimato são discussões relacionadas a mais primária faceta da internet, proeminente desde seus primórdios. A importância do seu ideal é de tal maneira talhado ao propósito da internet, que muitas vezes é difícil dissociar essa característica tão fundante da *natureza* do espaço virtual. Acerca dessa natureza, para já projetar os impactos na produção normativa, Lawrence Lessig discute a questão ao ilustrar como uma criança pode ser passar por um adulto na rede dominada pelo anonimato.

Pois, enquanto no espaço real, é difícil esconder que você é uma criança, no ciberespaço, ocultar quem você é, ou mais precisamente, ocultar características sobre quem você é, é a coisa mais simples do mundo. O padrão no ciberespaço é o anonimato. E porque é tão fácil esconder quem é, é praticamente impossível que as leis e normas sejam aplicadas no ciberespaço. Para que essas leis se apliquem, é preciso saber que é uma criança com quem estamos lidando. Mas a arquitetura do espaço simplesmente não fornece essas informações. (LESSIG, 1999, p. 6 - traduzimos)

A necessidade de assegurar a liberdade de expressão é um dos fatores que explicam a essencialidade do anonimato na internet; nascida como ferramenta de conexão de grupos distintos e principalmente como um espaço de divulgação de conteúdo, sobretudo acadêmico (CARDON, 2012), o valor da liberdade é visto como o supedâneo jurídico para a internet se manter livre de censuras. Com isso, a história da internet começa com o nascimento de *chats*, fóruns e plataformas para proporcionar essa comunicação em que certificar a identidade real do usuário não era uma prioridade. Assim, a liberdade marca o fenômeno desde seus primórdios, a internet *é determinada* por características básicas de sua arquitetura<sup>7</sup>. Ao

(Internet Protocol), número único de cada computador, que pode ser manipulado e alterado por um usuário que detenha conhecimento técnico específico. Ao longo do artigo, se faz referência meramente ao comportamento dos usuários comuns.

<sup>&</sup>lt;sup>6</sup> Com o desenvolvimento de tecnologia financeira, é possível a realização de trocas em ativos financeiros, até autodenominados moedas, em frações de segundos, com pouco custo operacional, muitas vezes prescindindo de um terceiro para intermediar a relação, como o fenômeno da Bitcoin exemplifica. Apesar de ser cedo para definir seus contornos exatos, é uma tendência incontestável.

<sup>&</sup>lt;sup>7</sup> Ao longo de sua obra Lessig (2006) informa que arquitetura é o código que constrói a internet, seus recursos, sua estrutura, suas páginas, e todas as outras características que conformam essa rede.

mesmo tempo, faz o caminho inverso e *determina*, ou seja, serve como o parâmetro que influencia a construção das ferramentas que ali operam. Tudo isso produz consequências profundas nas relações jurídicas que podem advir das relações sociais que ocorrem na internet, e certamente impõe obstáculos para aplicação normativa que ali pretenda regular.

Interessante reforçar como o anonimato é fruto dessa ostensiva liberdade. Estamos diante de um sistema integrado em que é possível saber "que existem entidades por aí interagindo com ele, mas não sabe nada sobre quem são essas entidades. Enquanto no espaço real - e aqui está o ponto importante - o anonimato deve ser criado, no ciberespaço o anonimato é o dado". (LESSIG, 2006, p.45 – traduzimos). Ou seja, ao usufruir da liberdade insculpida na arquitetura da rede, as trocas e conexões ocorrem sem se certificar necessariamente quem que afirma ser, verdadeiramente o é.

Contextualizando aos tempos atuais, é possível perceber como a internet é um local dominado pelas situações em que é possível interagir sem se identificar. A facilidade de criação de perfis em redes sociais, um dos meios de interação mais populares e foco de implicações de todos os tipos, é o maior exemplo disso. O uso de nomes e imagens falsas em situações que o indivíduo busca se passar por outra pessoa, ou esconder sua verdadeira identidade, seja com o propósito de ludibriar os outros usuários, seja por um mero ato recreativo ou cômico, é um fenômeno extremamente recorrente.

Assim, o ato de representar outra pessoa na internet não pode ser classificado peremptoriamente como danoso ou não. O que é certo é que "dentro dessa categoria mais ampla de comportamento cibernético indesejável, há também (1) *cyberbullying*, (2) *ciberassédio* e (3) *cyberstalking*." (KOCH, 2016, p. 239 – traduzimos). Ou seja, certamente é dessa possibilidade que emergem os casos em que há uma transgressão da mera conduta restrita ao mundo digital e se materializa no mundo real de maneira negativa, muitas vezes criminosamente. Com isso, o *bullying* ou as diversas formas de assédio e perseguição, ganham o prefixo para demonstrar o meio por qual estão sendo perpetradas.

Quando se pensa no universo dos relacionamentos on-line é possível visualizar como existe um potencial danoso na prática do ocultamento da identidade. Para engajar ou iniciar um relacionamento, a prática é ainda mais conhecida, já que a pessoa pode construir um

perfil que entenda mais atraente na internet; há, inclusive, um termo específico para designar esse comportamento tão típico dos relacionamentos na era digital, *Catfish*.<sup>8</sup>

Em decorrência desse cenário, não são raros os casos noticiados de *catfishing* o que resulta em incalculáveis danos às pessoas iludidas, àquelas que têm suas fotos e nome usados, àquelas que são vítimas de extorsão ou qualquer das vertentes de *cyberbullying*, *ciberassédio*, *cyberstalking*. Porém, há casos em que a ameaça pode atingir outros patamares de lesividade e adentrar de vez à seara criminal, momento em que "pode se transformar em assalto, estupro e perseguição no mundo real" (KOCH, 2016, p. 247 – traduzimos). É a partir dessas hipóteses, contemplando essa possibilidade como uma referência para as proposições, que nos propomos analisar o problema.

# A SEGURANÇA E A CERTIFICAÇÃO DA IDENTIDADE NOS APLICATIVOS DE RELACIONAMENTO

Ao longo de décadas de existência, preservou-se na internet, ou sempre se procurou preservar, os citados valores iniciais que a conduziam a se tornar um espaço em que o anonimato é assegurado (em benefício da liberdade e privacidade dos internautas). Essa lógica afetou a criação de sites ou aplicativos, ou simplesmente *apps*, desenvolvidos mesclando os recursos conhecidos das redes sociais para criar uma plataforma para as pessoas busquem parceiros para encontros casuais ou relacionamentos.<sup>9</sup>

Há muito tempo, casos de problemas decorrentes do aplicativo já aparecem nas discussões do modo de operar dessas plataformas. Em 2012, após uma mulher ter sido violentada após um encontro marcado por meio do *Match.com* e o caso ter alcançado relativo destaque na mídia, os responsáveis por três sites de relacionamento se comprometeram a adotar um maior escrutínio dos perfis (KOCH, 2016, p. 244 – traduzimos). Escusado será

<sup>9</sup> Para se cadastrar no Tinder, por exemplo, pode-se usar a conta do Facebook, ou mesmo por um email do Google, sem maiores exigências quanto a informações pessoais, ou mesmo nenhuma forma de certificação da identidade, conforme se pode averiguar em sua plataforma, disponível no endereço: <a href="http://www.tinder.com/">http://www.tinder.com/</a>.

<sup>&</sup>lt;sup>8</sup> Conforme remete Koch (2016), termo popularizado após o filme homônimo retrata a história de Nev Schulman e a sua descoberta de que a pessoa com quem mantinha um relacionamento virtual não era quem por quem falava ser, muito menos tinha a aparência das fotos que exibia.

dizer que essas resoluções, que careciam de caráter vinculante, de nada serviram para coibir o problema, já que, anos depois, o assunto permanece relevante e as plataformas ainda operam da mesma forma simples que antes o faziam.

Mais recentemente, Hillary Flynn, Keith Cousins e Elizabeth Naismith Picciani em parceria com *Columbia Journalism Investigations* conduziram uma investigação para identificar qual é o papel dessas plataformas na identificação dos usuários. A investigação nasceu após alguns casos de mulheres que afirmaram terem mantido contato, por meio dessas plataformas, com indivíduos condenados por crimes de violação sexual, sem que soubessem, pois os próprios aplicativos não mantinham esse controle. Considerando-se que havia relatos de várias mulheres, que usavam de plataformas distintas, percebeu-se que havia um padrão: os aplicativos de relacionamentos permitem – ou melhor, não adotam medidas para averiguar – que condenados por estupro montem perfis e façam uso da plataforma para reproduzir tal comportamento. (FLYNN et al., 2019).

O fato de o *Match Group* ser o operador de uma grande parcela desses aplicativos e sites (no total controlam mais de 40 sites de relacionamentos, dentre esses os mais populares no Brasil como o Tinder), permitiu a investigação apurar resultados quase uniformes já que é unissona a característica dessas plataformas de não se comprometerem em fazer a checagem de histórico de condenação por crime de natureza sexual do usuário, ou mesmo a checagem da identidade dos usuários nas versões gratuitas do software. Com isso, o porta-voz do grupo é categórico ao assumir: "definitivamente existem criminosos sexuais registrados em nossos produtos gratuitos" (FLYNN et al., 2019 – traduzimos).

Foi apurado que, desde quando surgiram as primeiras denúncias de violação sexual de encontros vinculados a esses sites, compromissos públicos foram firmados para garantir que medidas seriam tomadas no sentido de dificultar o uso desse canal para permitir esse comportamento e fortalecer a autenticação da identidade. No curso dos anos, outros casos surgiram (apenas na investigação citada avaliaram mais de 150¹º), tais compromissos foram constantemente renovados, porém nenhuma medida que buscasse coibir foi efetivamente

<sup>&</sup>lt;sup>10</sup> Dentre esses, alguns que resultaram em efetiva condenação criminal, outros foram meramente notificados às plataformas (FLYNN et. al, 2019).

implementada.

Hoje em dia, daqueles sites controlados pelo grupo, apenas o próprio Match.com, em sua versão *premium*, faz a verificação no registro nacional de *sex offenders* (o *Dru Sjodin National Sex Offender Public Website*, ferramenta do governo americano que unifica o registro das condenações ocorridas nos estados da federação e determina níveis aos condenado, baseando-se em sua possibilidade de reincidir). Apesar disso, "há anos o site argumenta, perante a justiça, que não tem obrigação legal de realizar verificações de antecedentes e lutou contra a legislação estadual que exigiria que divulgasse se o faz." (FLYNN et al., 2019 – traduzimos)

Mesmo se considerado o protocolo de banir o usuário, existe uma inoperância geral do sistema, que remete ao nosso problema principal: com a reiterada facilidade de ingressar com perfis falsos, o mero banimento do usuário não o impede de retornar a plataforma com dados inventados. Acerca disso, anota-se na matéria:

Os moderadores da empresa adotam uma mentalidade geral de "banir primeiro" para qualquer usuário acusado, mas uma vez bloqueados, eles têm pouca capacidade de impedir que o acusado use informações de identificação diferentes ou se inscreva em novas contas. Algumas dizem que se queixaram desse problema aos supervisores do OkCupid, apenas para serem ignoradas. Outras dizem que se viram pesquisando listas de criminosos por conta própria. (FLYNN et al., 2019 – traduzimos)

Em síntese, as histórias e os detalhes da investigação ajudam na construção do problema jurídico afundo que aqui se propõe a estudar: a internet propicia um conflito entre a privacidade, a liberdade de expressão, ambos correlatos ao propalado anonimato e, em oposição, a necessidade de se assegurar a segurança dos usuários, de maneira que o regulador enfrenta dificuldades ao conciliar de maneira efetiva os direitos sem que um não diminua o outro.

Ao final, o que o estudo mencionado sugere é que em um ambiente desenvolvido para facilitar o engajamento entre as pessoas a mulher se sentiria mais segura, em tese, para iniciar um relacionamento; contudo essa segurança é absolutamente falsa e a ausência de maior controle dessas plataformas apenas a coloca em situação de vulnerabilidade, assim, se torna

uma presa fácil para um criminoso que pode explorar essa ferramenta para ter uma facilidade que dificilmente teria no plano físico. Veja-se: uma mulher cadastrada no site de relacionamento certamente estaria mais inclinada a iniciar uma conversa e, eventualmente, marcar um encontro, já que se cadastrou no site, *exatamente* com esse propósito. Na vida real, a tarefa do explorador seria mais trabalhosa para encontrar uma situação social que assim a colocaria tão aberta às novas pessoas. A situação se torna ainda mais complexa, e certamente mais perigosa, quando se acrescenta o fator do anonimato, que permite a ação do criminoso em potencial ser ainda mais fácil, já que é outra arma dificultada no plano físico. Por mais que no mundo real ele poderia potencialmente se passar por outra pessoa, com outro nome e outra profissão, não conseguiria esconder seu rosto, um dos mais essenciais atributos de identidade, do ponto de vista social. Por isso, é imperativo concluir que "o anonimato dos aplicativos facilita que os infratores se tornem estupradores em série ao toque de um botão. Essa facilidade é auxiliada por possíveis vítimas não pensarem no ofensor como um estranho, mas como alguém que ele ou ela ficou conhecendo" (MURPHY, 2017, p.12).

Contudo, fazer a conexão entre o uso da plataforma e um suposto aumento dos casos de estupro e abuso sexual não é uma tarefa simples – nem é o argumento aqui estudado. Não há dados suficientes que permita afirmar categoricamente que o uso dessas plataformas exponencie a atuação criminosa – até porque, o crime de estupro apenas será concretizado na dimensão física, apesar de outros tipos de violência sejam passíveis de serem cometidos virtualmente, como os citados *cyberstalking*, *cyberbullying* e *ciberassédio*. Contudo, não é necessário fazê-lo para compreender os problemas aqui abordados. Outros fatores e algumas observações empíricas podem ser examinados para se construir um panorama do fenômeno no todo. Vejamos.

Lee (2019), ao fazer uma avaliação sociológica de todo o fenômeno dos relacionamentos virtuais, observa elementos que reforçam o que define como uma cultura misógina no ambiente virtual. Representada, sobretudo pela valoração da imagem, essa cultura contribui para o desequilíbrio no tecido social e significa que aplicativos como o Tinder se tornam um campo favorável para cultivo de ideais contrários à igualdade e que podem favorecer, em situações extremas, a manutenção de índices de violência física e

estupro. Thompson (2018), por sua vez, faz menção à ideia do *marketplace* e da teoria econômica para explicar a visão das mulheres como o produto nesse contexto, razão pela qual são constantemente tratadas de forma misógina e subserviente. A autora, inclusive, analisa extratos de conversas em que os homens adotam a postura violenta e reafirmam a pretensa superioridade enquanto gênero ao, por exemplo, subjugarem-nas por usarem sites de relacionamento (THOMPSON, 2018, p.83).

Parte da dificuldade de se fazer uma conexão direta é resultado do fato de os crimes de natureza sexual serem tradicionalmente subnotificados<sup>11</sup>; com isso, os dados obtidos pelas forças policiais certamente não refletem o número real de casos, carecendo igualmente dos detalhes da situação que o levou a ocorrer. Sem uma estatística que apresente a realidade com maior precisão, prejudica-se, via de consequência, a análise e o planejamento das estratégias mais eficientes para o combate – exatamente por ignorar uma parcela da análise que seria necessária na dimensão sociológica e imergir com mais precisão nas causas e estímulos sociais desse comportamento.

Ainda assim, verificou-se que em cinco anos, entre 2014 e 2018, ocorreu um aumento de 250% dos casos de violência relacionados ao Tinder, no estado de São Paulo. Foram 338 boletins, informado crimes como difamação, injúria, ameaça, estupro, extorsão, furto ou lesão corporal, todos de ocorrências registradas após encontros marcados por meio de aplicativos como Tinder, Badoo, Plenty of Fish, Happn ou Grindr (FERREIRA, 2019). O relato dos casos por trás dos números demonstra a existência de uma cultura de autoritarismo masculino que leva à violência e ao assédio. Contudo, há de se registrar, não é possível abstrair dos números quais foram resultado de perfis enganosos, quais tenham sido cometidos por agressores reincidentes, ou tenham sido casos avulsos que nem a mais rigorosa certificação de identidade poderia impedir.

Evidentemente, suprimir o direito daqueles condenados por estupro, ou que meramente tenha antecedentes, como o foco da investigação propôs, levanta um debate constitucional próprio, que foge ao escopo da presente reflexão. Mas, é possível pensar em

<sup>&</sup>lt;sup>11</sup> Característica reforçada no Dossiê Mulher 2019, produzido pelo Instituto de Segurança Pública do Rio de Janeiro (MANSO, CAMPAGNAC, 2019).

medidas que possam coibir esses casos, pensando tão somente no anonimato? É o que deve ser avaliado.

#### CONFLITO DE DIREITOS E MEDIDAS JURÍDICAS POSSÍVEIS

De acordo com dados das Nações Unidas, estima-se que 35% das mulheres já sofreram violência sexual ou de outra natureza; em alguns países, essa porcentagem pode chegar a 70%. A violência contra as mulheres é um óbice ao progresso e ao equilíbrio da sociedade. O combate constante a essa violência, seja em qualquer de suas vertentes, praticada por qualquer meio, ou em qualquer forma, é fundamental para uma sociedade que se proclama igualitária e democrática.

Portanto, como fica evidente a urgência e a distinção do problema, voltemos nossos olhos ao papel dos sites e aplicativos, especialmente na coibição dos perfis falsos. Pensando na internet como um todo, Lessig, reafirma a teoria da arquitetura e fornece as lições para compreender como a relação jurídica com o anonimato da internet é complexa.

Essa diferença nas arquiteturas do espaço real e do ciberespaço faz uma grande diferença na regulabilidade do comportamento de cada uma. A ausência de fatos relativamente autoaplicáveis no ciberespaço torna extremamente difícil regular o comportamento lá. Se todos pudéssemos andar como "O Homem Invisível" no espaço real, o mesmo aconteceria com o espaço real. O fato de não sermos capazes de nos tornar invisíveis no espaço real (ou pelo menos não facilmente) é um motivo importante para que a regulamentação possa funcionar. Assim, por exemplo, se um Estado deseja controlar o acesso das crianças ao discurso "indecente" na Internet, a arquitetura original da Internet fornece pouca ajuda. O Estado pode dizer aos sites: "não deixe as crianças verem pornografia". Mas os operadores do site não sabem - a partir dos dados fornecidos pelos protocolos TCP / IP - se a entidade que acessa sua página da web é uma criança ou um adulto. Isso é diferente, novamente, do espaço real. Se uma criança entra em uma loja de pornografia usando bigode e pernas de pau, é provável que seu esforço para ocultar falhe. O atributo "ser criança" é declarado no espaço real, mesmo que sejam possíveis esforços para ocultá-lo. Mas no ciberespaço, não é necessário ocultar, porque os fatos que você pode ocultar sobre sua identidade (ou seja, que você é crianca) não são declarados de qualquer maneira. Tudo isso é verdade, pelo menos, sob a arquitetura básica da

vol. 10, num. 29, 2020

<sup>&</sup>lt;sup>12</sup> Segundo estimativa apurada em estudo conduzido pela Organização Mundial da Saúde em conjunto com diversas entidades de Medicina e Saúde (WHO et. al., 2013).

Internet. Mas, como os últimos dez anos deixaram claro, nada disso é verdade por necessidade. Na medida em que a falta de tecnologias eficientes para autenticar fatos sobre indivíduos dificulta a regulação do comportamento, há arquiteturas que podem ser colocadas em camadas no protocolo TCP / IP para criar autenticação eficiente. Já estamos longe o suficiente da história da Internet para ver como essas tecnologias podem ser. Estamos bastante longe neste histórico para ver que a tendência para essa autenticação é imparável. A única questão é se incorporaremos neste sistema de autenticação os tipos de proteção necessários à privacidade e autonomia. (LESSIG, 2006, p. 45 – traduzimos)

Fica evidente com os apontamentos de Lessig que o problema eleva-se a um novo nível quando pensamos na autenticação: ainda que as plataformas cobrassem dos usuários dados pessoais, ou procedesse a investigação do histórico de condenações do indivíduo, ainda assim existiria uma barreira entre afirmar que quem está do outro lado da tela é o mesmo indivíduo identificado nos dados verificados. Porém, no problema aqui tratado, estamos em uma fase anterior a isso, em que sequer o mínimo das informações são requisitadas e é *ainda mais fácil* para a pessoa se omitir por trás da tela ostentando imagens e um nome diverso do real.

Portanto o primeiro passo que deve ser pensado é opor *alguma* dificuldade àquele que procura à plataforma online de encontro com propósitos escusos. De acordo com Koch (2016, p. 248) "os operadores de sites estão em uma posição única para impedir os danos causados nesses casos por comportamentos digitais indesejáveis." Koch lembra ainda Citron para reforçar:

Como os operadores de sites controlam o conteúdo exibido em seus sites, eles podem minimizar o dano removendo ou desindexando o abuso antes que ele se espalhe por toda a Internet. Eles podem moderar a discussão, adotar diretrizes claras para os usuários e suspender os privilégios dos usuários se assediarem os outros. (CITRON, 2014, p. 168 apud KOCH, 2016, p. 248— traduzimos).

Conforme identificado, essa possibilidade esbarra em outras proteções legais. Observando o caso dos perfis falsos nos estados Unidos, Koch (2016, p. 238) cita a Seção 230 do *Communications Decency Act* como o maior empecilho para os programadores e desenvolvedores dos aplicativos adotarem uma postura mais diligente no controle do conteúdo gerenciado pelos usuários, pois "concede ampla imunidade a operadores de sites para publicações prejudiciais de terceiros". Ainda, informa que mesmo nos estados que

criminalizam tal postura, há barreiras tecnológicas que torna a persecução criminal inviável e em geral, não produtiva. Todavia, apesar de não ter havido uma mobilização federal para implementar uma legislação que determinasse a checagem, há estados que demonstraram interesse em legislar sobre o tema.

No Brasil, qualquer análise legal deve partir da Constituição da República. Dentre as garantias elencadas, a CR/88 trouxe insculpido em seu artigo 5°, incisos IV e IX o direito fundamental a proteção do discurso, definindo em cada artigo, respectivamente que "é livre a manifestação do pensamento, sendo vedado o anonimato" e "é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença" (BRASIL, 1998). Na interpretação de Tavares, a proteção à liberdade de expressão pulverizada no texto constitucional leva a uma imprecisão do termo, que não deve ser confundido "é direito genérico que finda por abarcar um sem-número de formas e direitos conexos e que não pode ser restringido a um singelo externar sensações ou intuições, com a ausência da elementar atividade intelectual, na medida em que a compreende." (TAVARES, 2012, p. 627/628). Não protege, conforme a limitação expressa referida no inciso IV, o anonimato.

Embora as definições constitucionais sejam o ponto de partida de qualquer exploração normativa, é na legislação específica que devemos encontrar o supedâneo para nossa análise, nas normas que tratam das relações do mundo virtual. A lei 12.965/2014 (Marco Civil da Internet) contempla regras mais específicas, de conformidade com a legislação estabelecida fora do país, e foi responsável por um dos passos mais importantes para modernização da legislação no Brasil. A lei, em semelhança a seção 230 do dispositivo legal americano, contempla a mitigação da responsabilidade civil dos provedores de conteúdo pelo conteúdo produzidos pelos usuários da plataforma.

Art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.

Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as

#### disposições legais em contrário. (BRASIL, 2014)

Especificando ainda mais a análise, convém observar os termos de serviços dessas plataformas. Os termos do Tinder ilustram bem o que parece ser um padrão geral: a previsão expressa de exclusão da própria responsabilidade pelas condutas dos usuários.

Embora o Tinder se esforce para incentivar uma experiência de usuário com respeito, por meio de recursos como a dupla aceitação, que permite aos usuários se comunicarem apenas se ambos tiverem interesse um pelo outro, não somos responsáveis pela conduta do usuário dentro ou fora do Serviço. Você concorda em agir com cautela em todas as interações com outros usuários, especialmente ao decidir se comunicar fora do Servico ou pessoalmente. Além disso, você concorda em revisar e seguir as Dicas de segurança do Tinder antes de utilizar o Serviço. Você concorda que não fornecerá suas informações financeiras (p. ex., cartão de crédito ou informações de conta bancária) e que não transferirá ou enviará dinheiro por outros meios a outros usuários. VOCÊ É O ÚNICO RESPONSÁVEL POR SUAS INTERAÇÕES COM OUTROS USUÁRIOS. VOCÊ COMPREENDE QUE O TINDER NÃO INVESTIGA OS ANTECEDENTES CRIMINAIS DOS USUÁRIOS, NEM VERIFICA O HISTÓRICO DOS USUÁRIOS. O TINDER NÃO MANIFESTA DECLARAÇÕES OU GARANTIAS EM RELAÇÃO À CONDUTA DOS USUÁRIOS. O TINDER RESERVA-SE AO DIREITO DE CONDUZIR - E VOCÊ CONCORDA QUE O TINDER PODERÁ CONDUZIR -QUALQUER INVESTIGAÇÃO DE ANTECEDENTES CRIMINAIS OU DEMAIS VERIFICAÇÕES (COMO PESQUISAS EM REGISTROS DE CRIMINOSOS SEXUAIS) A QUALQUER MOMENTO, UTILIZANDO OS REGISTROS PÚBLICOS DISPONÍVEIS.(TINDER, 2018)

O panorama da legislação colacionada permite algumas conclusões. Conforme a investigação de Flynn, Cousins e Picciani indicou, bem como uma breve pesquisa em outros três sites populares no Brasil (além do Tinder, colacionado acima, define-se de maneira semelhante no Badoo, Be2 e Par Perfeito conforme seus respectivos termos de serviços) as configurações são semelhantes para todas as plataformas: não se responsabilizam pela conduta do usuário, bem como se reservam no direito de não de conduzir qualquer investigação a respeito dos antecedentes criminais. Nem se menciona a possibilidade de verificar a identidade dos usuários que se registram, por meio da exigência de algum documento pessoal ou algo semelhante. Essa posição é amparada pela direção estampada na legislação: preserva-se a liberdade, às plataformas é assegurada a ausência de

responsabilidade que as permite crescer e prosperar. Com isso, as vãs promessas de maior escrutínio continuam a ecoar a cada novo caso, sem qualquer indício de serem impostas.

Koch (2106, p. 252) sugere que os sites possuem poucos incentivos para efetivamente fiscalizar tal comportamento, pois, o número absoluto de perfis criados na plataforma, ou seja, quantificados ai os falsos, é um indicativo do sucesso que impacta diretamente na viabilidade financeira do projeto. Inclusive nos Estados Unidos há precedentes de supressão da responsabilidade para casos de perfis falsos (KOCH, 2016, p. 256).

A incapacidade de fornecer uma plataforma legitimamente segura e evitar esses casos fomenta uma inciativa dos usuários para se prevenirem. A criação de grupos de mulheres para compartilhar histórias e identificar agressores é uma forma que se manifesta a independência do público no papel de controle. Conforme lembra Thompson (2018), *Tinder Nightmares*, *Bye Felipe*, são exemplos de grupos formados por mulheres com o propósito de socializar as experiências, expor os agressores e eventualmente evitar que outras mulheres sejam vítimas de situações semelhantes pelos mesmos usuários.

Porém, algumas situações ultrapassam o limite do razoável, como o caso do ex-policial australiano Adrian Moore, que usou da prerrogativa de acesso aos registros da polícia para verificar os antecedentes criminais das mulheres com quem se conectava no Tinder (HALES, 2019). Além disso, o ex-policial é acusado de ter abusado sexualmente de mais de 100 mulheres que conheceu por meio dos aplicativos (KAUAR, MENAGH, 2020).

Por certo o problema é complexo e expõe as maiores dificuldades da interação no mundo digital. Sobrepesando todas as variáveis, reforça Koch:

Dada a dificuldade de criar medidas preventivas para impedir a criação de perfis falsos, perfis de imitações, e outros crimes cibernéticos não podem ser evitados de maneira eficaz; em vez disso, um site ou vítima deve aguardar a ocorrência do problema ou violação dos termos de serviço para tomar uma ação. Além disso, uma vez que um perfil falso é criado, as redes sociais têm pouco incentivo para impedi-los. (KOCH, 2016, p. 251 – traduzimos)

Poder-se-ia argumentar, do contrário, que exigir uma regulamentação maior seria impor uma obrigação que tornaria a legislação excessivamente paternalista; o ideal, para preservação da privacidade, segundo aqueles que argumentam pela proteção da liberdade,

seria educar os usuários a manterem uma conduta diligente quando usando essas plataformas. Já é essa previsão de cautela, que também define os termos de serviço consultados. Essa forma de visualizar a situação, embora seja sustentável por preceitos jurídicos válidos, despreza a sensibilidade que o caso demanda. Conquanto a liberdade deva ser, de fato, preservada, mais fundamental é a proteção da vida e integridade física da parcela dos indivíduos que usam da plataforma. Estamos diante de um fato em que uma mínima intervenção poderia resultar em um aumento da segurança e consequente diminuição de casos dessa natureza.

Essa discussão, acerca da necessidade de uma maior autenticidade nas relações pela internet, deve ser retomada nesse momento para que acompanhe as mudanças que ocorrem nas relações de privacidade e informações na internet. Ao redor do mundo são editadas legislações que buscam oferecer o supedâneo para aqueles que lidam com dados pessoais no contexto da internet. No Brasil, a lei nº 13.709, aprovada em 2019, é o mecanismo legal que nasce com o propósito de "de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (BRASIL, 2019). Em termos gerais, a legislação foi necessária para, dentre outros motivos, impedir o uso das informações fornecidas pelos usuários dos serviços virtuais de forma alheia a seu consentimento, como, por exemplo, para direcionar publicidade. O caso aqui discutido, embora tenha um contorno próprio, além ao alcance da referida legislação, tangencia à temática que ali é normalizada e, inclusive, pode ser um argumento que incentive a adoção de práticas que suprimam o anonimato. Com a garantia legal de que os dados pessoais serão mais bem protegidos pelas empresas e aplicativos, esvai-se a eventual preocupação do usuário de informar a plataforma informações verdadeiras quando preenche seu perfil.

Casos assim, em que a própria plataforma foi diligente na colheita de informações e checagem, não seriam inéditos. Na investigação apresentada nessa pesquisa, dois exemplos saltam aos olhos: o *True.com* e o extinto *Gatsby*, ambos rivais dos sites operacionalizados pelo Match Group, que se propuseram a manter um escrutínio maior nos perfis criados (FLYNN et al. 2019). Em ambos os casos, as plataformas mostraram que é possível efetivar a política de checar os antecedentes criminais dos usuários sem afetar sua operacionalização.

No entanto, os problemas de anonimato e as outras dificuldades podem ser resolvidos pela entidade que detém as informações da conta - o operador do site. Esses operadores de sites também têm recursos significativos à sua disposição, tornando a responsabilidade de investigar contas prejudiciais da maneira mais eficiente por eles. (KOCH, 2016, p. 267 - traduzimos)

Em resumo, Koch (2016, p. 275) sugere a necessidade se revisar o atual panorama de responsabilização dos provedores dos sites, exatamente para garantir maior segurança, sobretudo às mulheres, maior parcela afetada. Contudo, reconhece que, dentre outros problemas, uma legislação nesse teor poderia esbarrar na proteção à liberdade de expressão (KOCH, 2016, p. 278). Um primeiro passo, corroborando com as ponderações de Koch, seria a exigência de uma mínima certificação do usuário, que embora não resolvesse a totalidade dos casos, já abriria as portas para pensar em outras soluções futuras para cada vez mais eficientemente coibir tais situações.

#### **CONSIDERAÇÕES FINAIS**

O desenvolvimento tecnológico é, sem dúvidas, um dos importantes traços da sociedade moderna e a internet cumpre um papel integrativo nunca antes experimentado, da qual apenas começamos a entender as consequências. Dessas novidades advêm consequências positivas, como a possibilidade de democratização do acesso à informação e à conectividade global, mas advêm também outras que ainda não somos capazes de categorizar, como a evidente alteração do conceito e da dimensão da privacidade aplicável ao mundo virtual.

Com a facilidade para nos conectarmos por meio de ferramentas de interação social, surgiram fenômenos provocados tipicamente pela possibilidade do anonimato na internet, como o fenômeno conhecido como "Catfish". Não tardou para que esse fenômeno provocasse efeitos indesejáveis: casos de mulheres que se tornaram vítimas de agressão física ou propriamente sexual, como resultado de terem sido enganadas pelos usuários, seja por não serem quem afirmavam ser, seja por serem já reincidentes em crimes dessa natureza, mas ainda assim usando dos serviços desses sites que promovem as conexões dos usuários sem

certificarem os antecedentes criminais dos usuários.

Observa-se que as mulheres estão particularmente vulneráveis no ambiente virtual de relacionamentos. Isso é traduzido nos fatos observados na investigação: 1) é corriqueiro o uso de informações falsas e criação de perfis *fakes*; 2) houve um efetivo crescimento nos casos reportados de agressão sexual oriundas de relacionamentos iniciados no ambiente virtual e possibilitados pelos aplicativos, provando a necessidade tomar medidas para coibir; 3) pouco é feito pelas plataformas para combater essa situação, o que possibilita, por exemplo, agressores reincidentes permanecerem com perfis ativos ou voltarem com dados falseados. As mulheres, como a parte tradicionalmente mais vulnerável nas relações, se tornam um alvo ainda mais propício para serem vitimadas.

De certo, boa parte das variados desafios provocados pela internet, sobretudo aqueles que mais afetam a organização jurídica da sociedade, ainda não possuem a menor perspectiva de solução. O frequente choque de valores proporcionado pela rede coloca em perspectiva como as relações sociais são complexas e regidas por valores diversos que devem ser preservados. Aqui se trabalhou um desses choques: o do anonimato e da segurança; se os usuários são livres para marcarem presença na internet e nisso falsearem suas identidades, há a imediata consequência de que as relações estabelecidas por meio da internet jamais poderão ser perfeitamente seguras.

Não cabe fazer uma proposição de maneira assertiva de quais medidas podem ser implementadas, ou qual seriam eficientes para conter os casos de agressão derivados de encontros marcados por meio de aplicativos de relacionamento; o que se pode fazer é uma reflexão de como há um caminho facilitado aos criminosos para fazê-lo como poderia ser obstruído com medidas simples de autenticação da identidade. Conquanto as ressalvadas dificuldades de implementar uma certificação que seja efetiva, as medidas aqui aventadas como a exigência de maiores informações pessoais, e eventualmente, determinando-se que os sites procedam a verificação do histórico dos usuários, poderiam ser os primeiros passos para a construção de um cenário mais seguro para as mulheres que se propuserem a usufruir dessas ferramentas.

#### REFERÊNCIAS

BRASIL. Constituição da República de 1988. Constituição da República Federativa do Brasil. Diário Oficial da União. Brasília, 05 out. 1988. Disponível em: <a href="http://www.planalto.gov.br/ccivil\_03/constituicao/constituicaocompilado.htm">http://www.planalto.gov.br/ccivil\_03/constituicao/constituicaocompilado.htm</a> Acesso em 19 mar. 2020.

BRASIL. Lei nº 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União. Brasília, 15 ago. 2018. Disponível em: <a href="http://www.planalto.gov.br/ccivil\_03/\_ato2015-2018/2018/lei/L13709.htm">http://www.planalto.gov.br/ccivil\_03/\_ato2015-2018/2018/lei/L13709.htm</a> Acesso em 19 mar. 2020.

BRASIL. Lei nº 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil\_03/\_Ato2011-2014/2014/Lei/L12965.htm. Acesso em: 02 mar. 2020.

CANDIDO, Marcos. Tinder e apps de encontro tem aumento de 250% em ocorrências policiais. **Universa**, 28 jun. 2019.Disponível em: <a href="https://www.uol.com.br/universa/noticias/redacao/2019/06/28/tinder-e-apps-de-encontro-tem-aumento-de-250-em-ocorrencias-policiais.htm">https://www.uol.com.br/universa/noticias/redacao/2019/06/28/tinder-e-apps-de-encontro-tem-aumento-de-250-em-ocorrencias-policiais.htm</a>> Acesso em 13 fev. 2020.

CARDON, Dominique. **Democracia na Internet**: Promessas e Limites. Tradução de Nina Vincent e Tiago Coutinho. Rio de Janeiro: Forense Universitária, 2012.

CAVNA, Michael. "Nobody knows you're a dog": as iconic internet cartoon turns 20, creator peter Steiner knows the joke tings as relevant as ever. **Washington Post**, Jul. 2013. Disponível em: <a href="https://www.washingtonpost.com/blogs/comic-riffs/post/nobody-knows-youre-a-dog-as-iconic-internet-cartoon-turns-20-creator-peter-steiner-knows-the-joke-rings-as-relevant-as-ever/2013/07/31/73372600-f98d-11e2-8e84-c56731a202fb\_blog.html> Acesso em 24 mar 2020.

CHAPOLA, Ricardo. Estupradores usam aplicativos de namoro para atacar mulheres. **Folha de S. Paulo,** São Paulo, 27 set. 2017. Disponível em: <a href="https://www1.folha.uol.com.br/cotidiano/2017/09/1922031-estupradores-usam-aplicativos-de-namoro-para-atacar-mulheres.shtml">https://www1.folha.uol.com.br/cotidiano/2017/09/1922031-estupradores-usam-aplicativos-de-namoro-para-atacar-mulheres.shtml</a> Acesso em 13 fev. 2020.

MANSO, Flávia Vastano (Org.), CAMPAGNAC, Vanessa (Org.). **DOSSIÊ MULHER 2019**. Rio de Janeiro: RioSegurança, 2019. Disponível em: <a href="https://assets-dossies-ipg-v2.nyc3.digitaloceanspaces.com/sites/3/2019/05/ISP\_RJ\_DossieMulher\_2019.pdf">https://assets-dossies-ipg-v2.nyc3.digitaloceanspaces.com/sites/3/2019/05/ISP\_RJ\_DossieMulher\_2019.pdf</a> Acesso em 19 mar. 2020.

DROUIN, Michelle et. al.. Why do people lie online? "Because everyone lies on the internet". **Computers In Human Behavior**, [s.l.], v. 64, p.134-142, nov. 2016. Elsevier BV. Disponível em: <a href="http://dx.doi.org/10.1016/j.chb.2016.06.052">http://dx.doi.org/10.1016/j.chb.2016.06.052</a>. Acesso em 30 mar. 2020.

FERREIRA, Lola. A punição pelo desejo: registros de crimes relacionados a apps de relacionamento aumentaram mais de 250% em cinco anos. **Gênero e Número**. 23 mai. 2019. Disponível em: <a href="http://www.generonumero.media/punicao-desejo-crimes-apps-tinder-relacionamento/">http://www.generonumero.media/punicao-desejo-crimes-apps-tinder-relacionamento/</a> Acesso em 24 mar. 2020.

FLYNN, Hillary; COUSINS, Keith; PICCIANI, Elizabeth Naismith. Tinder Lets Known Sex Offenders Use the App. It's Not the Only One. **ProPublica**, 2 dez. 2019. Disponível em: <a href="https://www.propublica.org/article/tinder-lets-known-sex-offenders-use-the-app-its-not-the-only-one">https://www.propublica.org/article/tinder-lets-known-sex-offenders-use-the-app-its-not-the-only-one</a> Acesso em 17 dez. 2019.

HALES, Holly. Ex-cop jailed for looking up dozens of women he found on Tinder in police database - and fined \$2,000 for possessing bestiality pornography

**Daily Mail**, fev. 2019. Disponível em: <a href="https://www.dailymail.co.uk/news/article-6656413/Ex-cop-Adrian-Moore-jailed-looking-dozens-women-Tinder-police-database.html">https://www.dailymail.co.uk/news/article-6656413/Ex-cop-Adrian-Moore-jailed-looking-dozens-women-Tinder-police-database.html</a> Acesso em 13 fev. 2020

KAUAR, Herlyn; MENAGH, Joanna. Former WA Police officer Adrian Moore faces 108 sexual offences including drugging and raping women. **ABC News**, 4 mar. 2020. Disponível em: <a href="https://www.abc.net.au/news/2020-03-05/former-wa-police-officer-accused-of-more-than-100-sex-offences/12028052">https://www.abc.net.au/news/2020-03-05/former-wa-police-officer-accused-of-more-than-100-sex-offences/12028052</a> Acesso em 30 mar. 2020.

KOCH, Colleen M. To catch a catfish: a statutory solution for victims of online impersonation. **University of Colorado Law Review**, [s.l.], v. 88 n. 1, p. 233-280, 2017. Disponível em: <a href="http://lawreview.colorado.edu/wp-content/uploads/2017/01/12.-88.1-">http://lawreview.colorado.edu/wp-content/uploads/2017/01/12.-88.1-</a> Koch FinalRevised.pdf> Acesso em 30 mar. 2020.

LEE, Jin. Mediated Superficiality and Misogyny Through Cool on Tinder. **Social Media** + **Society**, [s.l.], v. 5, n. 3, p.1-11, jul. 2019. SAGE Publications. Disponível em: <a href="http://dx.doi.org/10.1177/2056305119872949">http://dx.doi.org/10.1177/2056305119872949</a>> Acesso em 18 mar. 2020.

LESSIG, Lawrence. The Zones of Cyberspace. Stanford Law Review, [s.l.], v. 48, n. 5, p. 1403-1467, Mai. 1996. Disponível em: <a href="https://www.jstor.org/stable/1229391?seq=1">https://www.jstor.org/stable/1229391?seq=1</a> Acesso em 18 mar. 2020

LESSIG, Lawrence. The law of the horse: what cyberlaw might teach. **Harvard Law Review**. [s.l], n. 113, p. 501- 546, 1999. Disponível em: <a href="https://cyber.harvard.edu/works/lessig/LNC\_Q\_D2.PDF">https://cyber.harvard.edu/works/lessig/LNC\_Q\_D2.PDF</a>> Acesso em 30 mar. 2020.

LESSIG, Lawrence. Code 2.0. New York: Basic Books, 2006.

MURPHY, Alyssa. Dating Dangerously: Risks Lurking within Mobile Dating Apps. **The Catholic University Journal of Law & Tech**, [s.l.], v. 26, n.1, p. 1-27, 2017. Disponível em:

<a href="https://pdfs.semanticscholar.org/affb/ace914boddae245e093f37faaff394cc7653.pdf?\_ga=2.227405533.1782641125.1589304667-2030659348.1589304667">https://pdfs.semanticscholar.org/affb/ace914boddae245e093f37faaff394cc7653.pdf?\_ga=2.227405533.1782641125.1589304667-2030659348.1589304667> Acesso em 25 mar. 2020.

TAVARES, André Ramos. **Curso de Direito Constitucional**. 10. ed. rev. e atual. – São Paulo : Saraiva, 2012.

TERMOS DE SERVIÇO DO BADOO. Badoo. 29 abril 2020. Disponível em <a href="https://badoo.com/pt/terms/">https://badoo.com/pt/terms/</a> Acesso em 19 ago. 2020.

TERMOS DE SERVIÇO DO BE2. Be2. 25 junho 2020. Disponível em: <a href="https://www.be2.com.br/info/termos-e-condicoes-de-servico">https://www.be2.com.br/info/termos-e-condicoes-de-servico</a> Acesso em 19 ago. 2020.

TERMOS DE SERVIÇO DO PAR PERFEITO. Par Perfeito. 06 junho 2019. Disponível em:<a href="https://www.parperfeito.com.br/registration/membagr.aspx?lid=4">https://www.parperfeito.com.br/registration/membagr.aspx?lid=4</a> Acesso em 19 ago. 2020.

TERMOS DE SERVIÇO DO TINDER. **Tinder**. 09 maio 2018. Disponível em: <a href="https://www.help.tinder.com/hc/pt-br/articles/360003040592-Termos-de-Servi%C3%A70">https://www.help.tinder.com/hc/pt-br/articles/360003040592-Termos-de-Servi%C3%A70</a> Acesso em 13 fev. 2020.

THE UNITED STATES DEPARTMENT OF JUSTICE. **Dru Sjodin National Sex Offender Public Website**. Página inicial. Disponível em: <a href="https://www.nsopw.gov/">https://www.nsopw.gov/</a> Acesso em 19 ago. 2020.

THOMPSON, Laura. "I can be your Tinder nightmare": Harassment and misogyny in the online sexual marketplace. **Feminism & Psychology** 2018, Vol. 28 (1) 69–89. Disponível em: <a href="https://journals.sagepub.com/doi/full/10.1177/0959353517720226">https://journals.sagepub.com/doi/full/10.1177/0959353517720226</a>. Acesso em 24 mar. 2020.

WORLD HEALTH ORGANIZATION et. al. **Global and regional estimates of violence against women:** prevalence and health effects of intimate partner violence and non-partner sexual violence. Genebra, 2013. Disponível em: <a href="https://apps.who.int/iris/bitstream/handle/10665/85239/9789241564625\_eng.pdf">https://apps.who.int/iris/bitstream/handle/10665/85239/9789241564625\_eng.pdf</a>; jsessio nid=5260C656F1383CAFEA2E650ABB7B0822? sequence=1> Acesso em 30 mar. 2020.