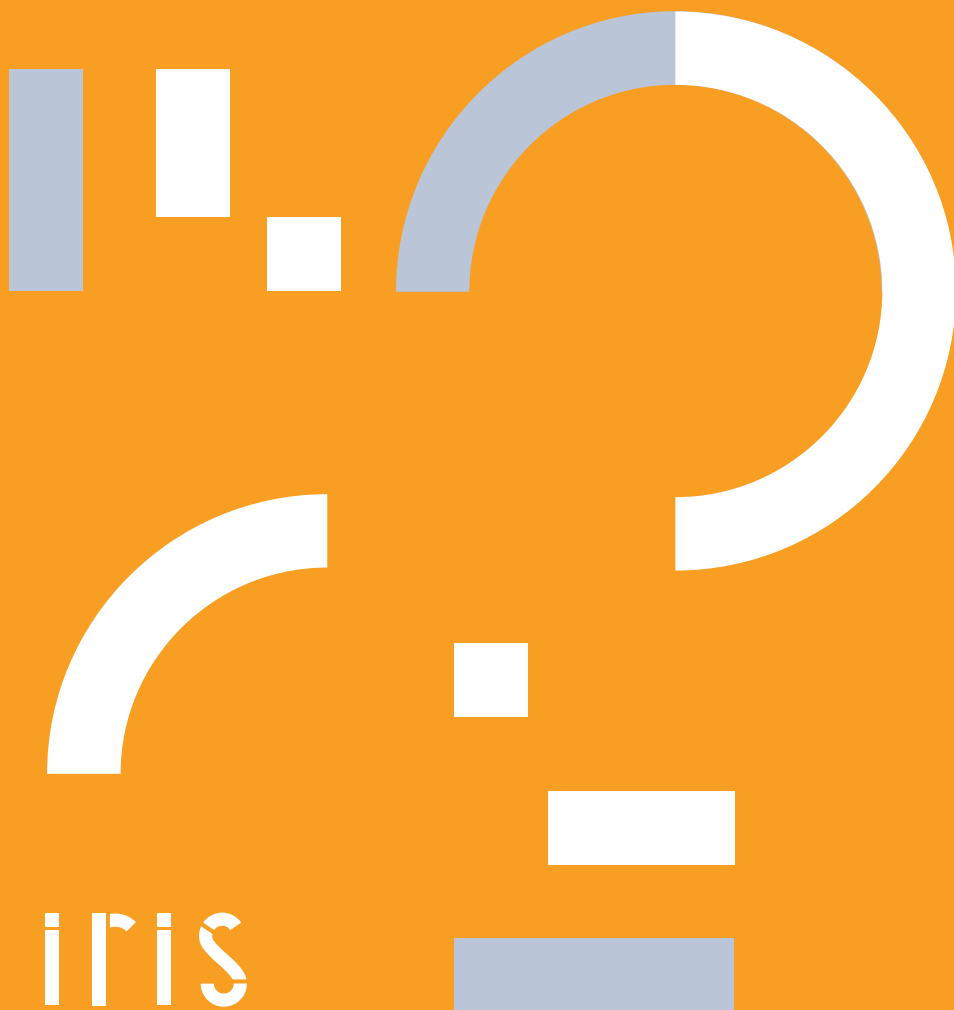


# 2

## glossário da **Inclusão Digital**

- Problemáticas
- Sociedade da Informação



# glossário da **Inclusão Digital** vol. 2

## **AUTORIA**

Ana Bárbara Gomes  
Felipe Duarte  
Paloma Rocillo

## **CONSELHO CIENTÍFICO**

Lucas Costa dos Anjos

## **PROJETO GRÁFICO E CAPA**

Felipe Duarte

## **DIAGRAMAÇÃO E FINALIZAÇÃO**

Felipe Duarte

## **PRODUÇÃO EDITORIAL**

Instituto de Referência em Internet e Sociedade

## **REVISÃO**

Lucas Costa dos Anjos  
Luíza Brandão

## **COMO CITAR EM ABNT**

CARMO, Paloma; DUARTE, Felipe; GOMES, Ana Bárbara.  
**Glossário da Inclusão Digital - Volume II.** Instituto de  
Referência em Internet e Sociedade: Belo Horizonte, 2020.  
Disponível em: <<http://bit.ly/3aqUlfP>>. Acesso em: dd mmm.  
AAAA.

G633 Gomes, Ana Bárbara.

Glossário da inclusão digital : vol. 2 [recurso  
eletrônico] / Ana Bárbara Gomes, Felipe Duarte e Paloma  
Rocillo. —Belo Horizonte : IRIS, 2020.  
Dados eletrônicos (pdf).

"Problemática; Sociedade da informação" [retirado da  
capa]

Inclui bibliografia.  
ISBN 978-85-94202-06-2

1. Sociedade da informação. 2. Comunicações digitais.  
3. Internet – Aspectos morais e éticos. I. Duarte, Felipe.  
II. Rocillo, Paloma. III. Título.

CDD 303.4833



Esta obra foi publicada nos  
termos da licença  
Atribuição- não comercial 4.0  
internacional  
<[https://creativecommons.org/  
licenses/by-nc/4.0/](https://creativecommons.org/licenses/by-nc/4.0/)>

# iris

INSTITUTO  
DE REFERÊNCIA  
EM INTERNET  
E SOCIEDADE

**DIREÇÃO**

Luíza Couto Chaves Brandão

**VICE-DIREÇÃO**

Odélio Porto Jr.

**CONSELHEIROS CIENTÍFICOS**

Fabício Bertini Pasquot Polido

Lucas Costa dos Anjos

**MEMBROS**

Ana Bárbara Gomes / Pesquisadora

Anna Célia Carvalho / Comunicação

Felipe Duarte / Comunicação

Gustavo Rodrigues / Pesquisador

Lahis Kurtz / Pesquisadora

Paloma Rocillo Rolim do Carmo / Pesquisadora

Pedro Vilela Resende Gonçalves / Co-fundador e pesquisador

Victor Barbieri Rodrigues Vieira / Pesquisador

# SUMÁRIO

INTRODUÇÃO	8
------------	---

METODOLOGIA	12
-------------	----



1. SOCIEDADE DA INFORMAÇÃO	17
----------------------------	----

1.1 Governança da internet	20
1.2 Capital informacional	23
1.3 Comunidade digital	24
1.4 Atenção profunda / hiperatenção	25
1.5 Clausura digital	25
1.6 Governo eletrônico	26
1.7 Ética digital	27
1.8 Gerações tecnológicas	27
1.9 Imersão digital	28
1.10 Imigrantes digitais	28
1.11 Nativos digitais	29
1.12 Plataformas digitais	30
1.13 Privacidade	32
1.14 Proteção de dados	36
1.15 Provedor de internet	38
1.16 Mídias sociais	39
1.17 Sociedade digital	40
1.18 TIC	40
1.19 Telecentro	41
1.20 Tecnopolítica	41
1.21 Transculturalidade	43
1.22 Web 2.0	44
1.23 Moderação de conteúdo	44



## **2. PROBLEMÁTICAS** **55**

2.1 Apropriação de tecnologias	<b>56</b>
2.2 Assédio on-line	<b>56</b>
2.3 Ciberbullying	<b>58</b>
2.4 Desinformação	<b>59</b>
2.5 Discurso de ódio	<b>62</b>
2.6 Exclusão digital	<b>63</b>
2.7 Fake news (“notícias falsas”)	<b>64</b>
2.8 Processo de inclusão excludente	<b>65</b>
2.9 Aliciamento on-line	<b>66</b>
2.10 Phishing e golpes	<b>68</b>
2.11 Sexting	<b>70</b>
2.12 Cyberstalking	<b>70</b>
2.13 Uso excessivo da internet	<b>72</b>
2.14 Controle parental	<b>74</b>
2.15 Pornografia de revanche	<b>75</b>
2.16 Anonimato	<b>76</b>
2.17 Superexposição	<b>77</b>
2.18 Vigilantismo	<b>78</b>

## **AUTORIA** **86**

## **BIBLIOGRAFIA** **88**

# PREFÁCIO



A ideia de inclusão digital está relacionada também a arranjos sociais, políticos, econômicos e culturais que se conectam à informação, comunicação e conhecimento. Emergem, então, diferentes contextos, oportunidades e desafios para que a internet seja usufruída não apenas como meio de comunicação, mas também - e especialmente - como direito. Por isso, buscamos reunir no segundo volume do Glossário da Inclusão Digital conceitos abarcados pela ideia de uma “sociedade da informação” e das situações que ainda exigem mais reflexão e debate, reunidas sob “problemáticas”.

O primeiro volume do Glossário apresentou conceitos relativos ao acesso, indicadores, marcos regulatórios brasileiros e competências digitais, a fim de oferecer oportunidades de diálogo para a academia, sociedade civil, legislativo e de políticas públicas. A receptividade da obra em diversos setores e espaços demonstrou o caleidoscópio pelo qual a inclusão digital deve ser observada na agenda brasileira. Assim, iniciativa de oferecer bases conceituais e semânticas para a consecução da inclusão digital no país continua neste segundo volume, também elaborado por Ana Bárbara Gomes, Felipe Duarte e Paloma Rocillo.

Juntos, os dois volumes do Glossário da Inclusão Digital resultam do projeto “Barreiras e desafios à inclusão no Brasil” do Instituto de Referência em Internet e Sociedade (IRIS). O projeto constitui-se como oportunidade para intervenção na realidade social, na medida em que aborda temas ainda pendentes de compreensão, apreensão e efetivação para a transformação digital e políticas correlatas. O Glossário conta com pesquisa documental, revisão bibliográfica e diálogo multidisciplinar e abre oportunidades para futuras reflexões sobre a inclusão, em suas interfaces digitais e sociais.

Belo Horizonte, janeiro de 2020

# INTRODUÇÃO





Em 2011, a ONU, por meio do relatório especial sobre a promoção e a proteção do direito à liberdade de opinião e de expressão<sup>1</sup>, declarou o acesso à internet como um direito humano. Conforme apontado pelo relator Frank La Rue<sup>2</sup>, a internet tem um potencial único para que indivíduos exerçam sua liberdade de expressão e opinião, contribuindo para o progresso da sociedade como um todo. Entretanto, para que isso se concretize, os comportamentos e motivações dos usuários da rede devem ser considerados.

O historiador Mark Poster afirma que a internet, além de tecnologia, é um espaço social<sup>3</sup>. A afirmação de Poster justifica-se pelos debates políticos, construção de conhecimento coletivo, divulgação de produções artísticas e outras atividades próprias da sociedade e do ímpeto humano que são manifestas na internet. Por ser uma rede de socialização, é compreensível que os comportamentos nocivos e agressivos praticados por indivíduos no mundo offline também sejam praticados no ambiente online. Sendo assim, é essencial o diálogo e a reflexão sobre como as relações online efetivam o uso da internet como ferramenta para a promoção de direitos e para o desenvolvimento pleno do potencial humano.

No volume 1 do Glossário para Inclusão Digital<sup>4</sup>, foram apresentadas definições de conceitos que são pressupostos para inclusão digital, de acordo com Cristina Mori<sup>5</sup>: i) acesso -

---

1 ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS. **Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue**. Nova York: Onu, 2011. Disponível em: <<https://bit.ly/2wtUFbk>>. Acesso em: 23 set. 2019.

2 Ibid, p. 1

3 POSTER, Mark. **CyberDemocracy: Internet and the Public Sphere**. Disponível em <<https://bit.ly/2kTjQ4G>>. Acesso em 23 ago. 2018

4 CARMO, Paloma; DUARTE, Felipe; GOMES, Ana Bárbara. **Glossário da Inclusão Digital** - Volume I. Instituto de Referência em Internet e Sociedade: Belo Horizonte, 2019. Disponível em: <<https://bit.ly/33aGTJb>>. Acesso em: 10 out. 2019.

5 Cristina Kiomi Mori, **Políticas públicas para inclusão digital no Brasil: aspectos**

que se relaciona a questões de infraestrutura; ii) alfabetização digital - desenvolvimento de habilidades que permitam o uso pleno das tecnologias da informação e comunicação (TICs); e iii) apropriação de tecnologias. Foram apresentados ainda conceitos como acessibilidade, usabilidade, Marco Civil da Internet, letramento digital, empoderamento comunicacional etc.

Na primeira seção deste Volume, apresentamos conceitos referentes a elementos próprios da sociedade da informação, considerada por Werthein<sup>6</sup> como o “principal traço característico do debate público sobre desenvolvimento, seja em nível local ou global, neste alvorecer do século XXI”. Na segunda seção reunimos problemas relacionados ao uso indevido da internet, que se refletem, inclusive, em crimes e violações contra os direitos humanos. Além disso, serão explanados conceitos relacionados aos desafios da promoção de inclusão digital em condições de precariedade.

As situações apresentadas a seguir servem de substrato para reflexões de atores da internet e para a consecução de estratégia de enfrentamento das problemáticas descritas. Portanto, este volume busca contribuir com educadores que promovem a aproximação de crianças e de adolescentes com a rede; de agentes de políticas públicas para regulação e universalização do acesso ao ambiente online no âmbito legislativo, executivo ou judiciário; e de todos usuários da rede mundial de computadores. Assim como proposto no primeiro volume deste glossário, não temos como objetivo esgotar a discussão sobre os temas, mas oferecer um aporte teórico que sirva de referência para os diversos atores incluídos na dinâmica digital.

Cada conceito apresentado neste glossário busca construir conhecimento e provocar análises sobre o atual cenário do uso

---

**institucionais e efetividade em iniciativas federais de disseminação de telecentros no período 2000-2010**, (2011). Disponível em <<https://bit.ly/2maPF97>>. Acesso em 10 set. 2019.

<sup>6</sup> WERTHEIN, Jorge. A sociedade da informação e seus desafios. **Ci. Inf., Brasília**, v. 29, n. 2, p. 71-77, 2000. Disponível em <<https://bit.ly/2lWfmdK>>. Acesso em 16 set. 2019

da internet. Para tanto, trabalhamos problemáticas e discussões importantes para caminhos que queremos trilhar para que a internet seja um efetivo instrumento de promoção de uma sociedade mais justa, igualitária e diversa.

**METODOLOGIA**



Para a definição dos eixos de composição do glossário, foram considerados os problemas de pesquisa delimitados no Projeto de Pesquisa Barreiras e Desafios à inclusão digital no Brasil: Instrumentos do Direito & Tecnologias para transformação da realidade social digital<sup>1</sup>. A metodologia utilizada para a escolha dos termos de composição deste volume do Glossário foi a mesma utilizada para a pesquisa dos termos que constam no Volume 1.<sup>2</sup>

Os problemas de pesquisa foram divididos em três blocos: i) conceitos; ii) práticas; e iii) indicadores. A partir de então, foram estabelecidos termos de pesquisa com o objetivo de fazer uma busca inicial sobre o estado da arte dos estudos científicos que tinham por objeto os problemas de pesquisa do Projeto<sup>3</sup>. A etapa seguinte consistiu em revisão sistemática de literatura utilizando a base de dados Scopus, por ser “o maior banco de dados de resumos e citações da literatura revisada por pares”<sup>4</sup>.

Esse procedimento foi realizado por pesquisadores do IRIS com o objetivo de garantir a homogeneidade na aplicação dos

---

**1** IRIS. **Projeto de Pesquisa Barreiras e Desafios à inclusão digital no Brasil:** Instrumentos do Direito & Tecnologias Para Transformação da Realidade Social Digital. Disponível em <<https://bit.ly/342Pe2p>>, acesso em 28 de ago. de 2019.

**2** CARMO, Paloma; DUARTE, Felipe; GOMES, Ana Bárbara. **Glossário da Inclusão Digital** - Volume I. Instituto de Referência em Internet e Sociedade: Belo Horizonte, 2019. Disponível em: <<http://irishh.com.br/publicacoes/glossario-da-inclusao-digital-volume-1/>>. Acesso em: 10 out. 2019.

**3** Os termos de pesquisa utilizados foram: i. “digital inclusion” AND “concept”; ii. “digital inclusion” AND “digital literacy” -OR- “digital inclusion” AND “media literacy” -OR- “digital literacy” AND “media literacy”; iii. “digital literacy” AND “citizenship” -OR- “digital literacy” AND “politics”; iv. “misinformation” AND “media literacy”; v. “public policies” AND “digital inclusion” -OR- “public policies” AND “hate speech” AND “online” -OR- “public policies” AND “misinformation”; vi. “media literacy” AND “strategy”; vii. “Programa inclusão digital” OR “Lei 11.021/04”; viii. “Plano Nacional da Educação” AND “technology”

**4** Para saber mais sobre o banco de artigos do Scopus acesse: <<https://bit.ly/2Zoupzx>>, acesso em 28 de ago. de 2019.

critérios para seleção de artigos e teve como objetivo verificar o estado da arte<sup>5</sup> das pesquisas sobre inclusão digital, além de verificar os termos mais recorrentes nas pesquisas sobre o tema em questão. Destaca-se que, nessa fase, foi realizada pesquisa exaustiva, ou seja, todos os resultados encontrados após aplicação dos termos de pesquisa foram analisados. Os artigos selecionados para comporem o corpo de pesquisa foram selecionados com base nos seguintes critérios: i) acesso aberto; e ii) temática pautada nas competência ou aplicações da inclusão digital, seja na sua dimensão estrutural, social ou política. A seguir, todos os artigos selecionados a partir da revisão sistemática foram lidos e, posteriormente, selecionadas as expressões ou vocábulos que fariam parte do glossário. Os critérios para escolha do vocabulário do glossário foram os seguintes: i) frequência, aqueles que apareceram com regularidade destacável entre os artigos coletados; e II) coerência, àqueles que nos pareceram relevantes para a compreensão do tema da inclusão digital.

Após exauridos todos os artigos selecionados a partir da revisão sistemática de literatura<sup>6</sup>, os termos de pesquisa selecionados foram buscados nas bases de dados Google Acadêmico<sup>7</sup> e Capes<sup>8</sup>. Essa fase, diferentemente da revisão

---

5 DE ALMEIDA FERREIRA, Norma Sandra. As pesquisas denominadas estado da arte. **Educação & sociedade**, v. 23, p. 257, 2002. Disponível em <<https://bit.ly/2Hyi5C2>>. Acesso em 12 de ago. de 2019

6 Revisão sistemática de literatura é um método meta-científico, ou seja, estudos sobre o funcionamento, explicação e validade da própria ciência. Os métodos meta-científicos são apontados como uma das maneiras para avaliação do conjunto da produção científica em uma determinada área do conhecimento. Para tanto, fontes de publicação científica, bases de indexação de dados, bancos de teses e dissertações, periódicos científicos são definidos como base para pesquisa exaustiva dos estudos desenvolvidos em determinada matéria. Com resultado, obtém-se a síntese das ideias e resultados no tema pré-definido, bem como o impacto da produção". WITTER, G. P. **Metaciência e psicologia**. Campinas: Alínea, 2005.

7 Para saber mais sobre o banco de artigos do Google Acadêmico acesse [https://scholar.google.com/schhp?hl=pt-BR&as\\_sdt=0,5](https://scholar.google.com/schhp?hl=pt-BR&as_sdt=0,5), acesso em 26 de ago. de 2019.

8 Para saber mais sobre o banco de artigos da Capes acesse: <http://www.periodicos>.

sistemática realizada no Scopus, não foi exaustiva, uma vez que seu objetivo não era compreender o estado da arte sobre o tema. Na verdade, buscou-se incorporar conceitos amplamente utilizados por teóricos e agentes de políticas públicas, além da pretensão de integrar conceitos recentes ao glossário. Foi necessário explorar outras bases de artigos, aplicando os mesmos termos de pesquisa, pois o Scopus abrange apenas artigos publicados nos periódicos nele cadastrados. Por essa razão, estudos de alta relevância não foram encontrados na pesquisa no Scopus. Após a busca dos termos de pesquisa nas bases do Google Acadêmico, Scielo e Capes, foram selecionados artigos para leitura de acordo com os seguintes critérios: i) acesso aberto; e ii) inclusão digital como tema central do artigo. Novamente, o procedimento foi realizado por pesquisadores do IRIS com o objetivo de garantir a homogeneidade na seleção de artigos. Os trabalhos selecionados foram lidos e foram escolhidas expressões e vocábulos para constituição do glossário.

Por fim, todos os vocábulos selecionados foram divididos em cinco grupos, concebidos a partir dos eixos derivados dos problemas constantes no Projeto de Pesquisa. Os grupos são: 1. acesso; 2. indicadores; 3. competências digitais; 4. diretrizes e marcos regulatórios; 5. sociedade da informação; e 6. problemáticas. Os vocabulários foram enquadrados de acordo com a pertinência temática a cada grupo. Cada grupo vocabular corresponderá a uma seção do glossário. O volume 1 compreende os grupos vocabulares de 1 a 4. Nesta publicação, o Volume 2, constam os termos encontrados nas seções 5. sociedade da informação e 6. problemáticas.

O objetivo desta pesquisa é descritivo, ou seja, tem como propósito “primordial a descrição das características de determinada população ou fenômeno ou o estabelecimento de relações entre variáveis”<sup>9</sup>. Para a formulação dos conceitos contidos neste volume, foi utilizado o método de pesquisa

---

[capes.gov.br/](http://capes.gov.br/), acesso em 26 de ago. de 2019.

<sup>9</sup> GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. Editora Atlas SA, 2008. Disponível em <<https://bit.ly/2kMjLiU>>. Acesso em 16 set. 2019.

bibliográfica, que é desenvolvido a partir de material científico disponibilizado pelos respectivos autores como livros e artigos científicos.



# **1. SOCIEDADE DA INFORMAÇÃO**



# 1. SOCIEDADE DA INFORMAÇÃO

Na sociedade da informação, a dinâmica social de interações, trabalho e comunicação são inteiramente permeadas por densos fluxos informacionais que ocupam posição central na rotina dos indivíduos. O conhecimento das informações é substrato importante para que a sociedade civil, empresas e governos norteiem suas decisões. O número de pessoas envolvidas em trabalhos relacionados ao manuseio de informações (desde a coleta e processamento, até o desenvolvimento de tecnologias que aprimoram manuseio) é maior do que em outros setores da sociedade. Ao escrever sobre informatização no novo milênio, Rogers<sup>1</sup> apresenta o cenário de países como EUA, Alemanha, Japão e Cingapura, onde pelo menos dois terços dos trabalhadores se concentram em profissões relacionadas à informação, como professores, jornalistas, grande parte do setor empresarial e profissionais da tecnologia da informação. Segundo o autor:

Em uma sociedade da informação, a informação é o ingrediente vital, como a energia estava na sociedade industrial e como o trabalho manual era na agricultura. O computador é para a

sociedade da informação  
o que a máquina a vapor  
era para a sociedade  
industrial.<sup>2</sup>

Castells (2000)<sup>3</sup> aponta algumas características imperativas para o que o autor chama de paradigma da tecnologia da informação, formulado por Carlota Perez, Christopher Freeman e Giovanni Dosi, e que ajuda a compreender a dinâmica entre tecnologia e inovação e suas implicações socioeconômicas. São eles: 1. A informação é sua matéria-prima: tecnologias são desenvolvidas para permitir acessá-la como fim último, em oposição ao que costumava ser o padrão, quando a informação era meio para o acesso à tecnologia. 2. A informação é parte integrante das atividades coletivas e individuais da sociedade e, portanto, as tecnologias passam a incidir diretamente no cotidiano que partilhamos e têm seus efeitos capilarizados. 3. Predomínio da lógica de redes: que é adequada ao aglutinado de informações e de interações que apontam neste tempo. 4. Flexibilidade: processos, organizações e instituições têm a característica de serem modificáveis e se transformarem repentinamente, sem grandes perdas. 5. Convergência de tecnologias específicas para um sistema altamente integrado: a modernização dos múltiplos processos os aproximam e cada vez mais tecnologias das mais distintas naturezas são integradas a um sistema de informação. Essas características funcionam como base material da sociedade da informação.

\* Diversos processos históricos, econômicos e sociais, incluindo o declínio do sistema político medieval, favoreceram para que em 1648, com o fim da Guerra dos Trinta anos, fossem acordados diversos tratados de reconhecimento da soberania e centralização do poder político de cada Estado. Essa série de tratados são conhecidos como Paz de Westfalia, consolidando o fim da hegemonia da Igreja e o surgimento da sociedade internacional moderna integrada por Estados iguais, independentes e soberanos.

COLOMBO, Silvana. ESTADO, SOBERANIA E PODER: UMA VISÃO A PARTIR DA SOCIEDADE INTERNACIONAL. Revista Argumentum-Argumentum Journal of Law, v. 8, p. 97-114, 2008. Disponível em <<https://bit.ly/2oB0ji4>>. Acesso em 30 out. 2019.

## 1.1. Governança da internet

Antes do advento da internet, o termo governança era quase que unicamente associado a Estado nacional. Essa concepção se justifica pela forma de surgimento do Estado Moderno, pautado no modelo westfaliano\*, em que a soberania nacional era característica primordial para nações. Logo, os atos que diziam respeito a condutas dos cidadãos eram decididos apenas pelo Estado.

Com a internet, a *Internet Engineering Task Force* (IETF), estabelecida em 1986, corroborou o avanço do desenvolvimento da internet. A IETF é “um grupo informalmente auto-organizado de pessoas que contribuem para a engenharia e evolução das tecnologias usadas na internet”<sup>4</sup>. O grupo adotou um processo de tomada de decisões baseado na cooperação e no consenso, em que não havia um governo central coordenando os trabalhos e padrões estabelecidos.

A Cúpula Mundial sobre Sociedade da Informação (CMSI), realizada em Genebra (2003) e em Túnis (2005), foi um marco para a abordagem descentralizada da governança da internet. A expressão governança da internet foi introduzida ao processo da CMSI durante a reunião regional da Ásia Ocidental em fevereiro de 2003. Essa interpretação colidiu com o significado mais amplo do termo ‘governança’, que inclui a governança dos assuntos de qualquer instituição, incluindo instituições não governamentais.

Em 2005, na CMSI de Túnis, foi criado o Fórum de Governança da Internet (IGF), um experimento para a diplomacia multissetorial. Nesse momento, construiu-se de maneira mais concreta a definição de governança da internet:

Governança da internet é o desenvolvimento e a aplicação pelos Governos, pelo setor privado e pela sociedade civil, em seus respectivos papéis, de princípios, normas, regras, procedimentos de tomadas de decisão e programas em comum que definem a evolução e o uso da internet<sup>5</sup>

Os processos multissetoriais se baseiam no reconhecimento da importância de alcançar equidade e assumir responsabilidades na comunicação entre os setores. Além disso, fundam-se em princípios democráticos de transparência e de participação<sup>6</sup>.

O modelo de governança da internet fundamenta o Comitê Gestor da Internet no Brasil (CGI.br)<sup>7</sup>, criado pela Portaria Interministerial nº 147 em 1995<sup>8</sup>. O CGI.br é responsável por estabelecer diretrizes sobre o uso da internet no Brasil, responsável pela alocação de Endereço IP e pela administração do Domínio de Primeiro Nível, “.br”, entre outras atribuições. O CGI.br é composto por 9 representantes do setor governamental, 4 do setor empresarial, 4 do terceiro setor, 3 da comunidade científica e tecnológica

e 1 representante de notório saber em assuntos de internet. O CGI.br é considerado pioneiro no mundo em relação ao modelo de governança da internet praticado, além de orientar suas ações e decisões segundo os seguintes princípios<sup>9</sup>:

1. Liberdade, privacidade e direitos humanos
2. Governança democrática e colaborativa
3. Universalidade
4. Diversidade
5. Inovação
6. Neutralidade da rede
7. Inimputabilidade da rede
8. Funcionalidade, segurança e estabilidade
9. Padronização e interoperabilidade
10. Ambiente legal e regulatório

O multissetorialismo do CGI.br está presente desde a origem do Comitê. Os membros do CGI.br são representantes de setores em específicos e eleitos a cada três anos, a partir dos votos de um colégio eleitoral. Conforme o Decreto 4.829, de 3 de Setembro de 2003, os setores da sociedade elegem seus respectivos representantes,

sendo que o setor empresarial tem o direito a 4 representantes no comitê, o mesmo número de que o terceiro setor dispõe. A comunidade científica elege 3 representantes, enquanto o setor governamental possui 9 cadeiras disponíveis dentro da instituição. Por fim, existe um representante de notório saber em assuntos da internet, indicado pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações.

A partir da estrutura anteriormente apresentada de formação do CGI.br, o Brasil institucionaliza um modelo de governança da internet pluriparticipativo, cuja concretização depende do diálogo entre os diferentes agentes que intervêm no funcionamento e uso da internet em direção ao comum objetivo de melhoria da qualidade de vida do cidadão por meio do uso das **TICs**.

## 1.2. Capital Informacional

Capital informacional diz respeito ao interesse e à motivação dos indivíduos para se engajar no processo de se informar. Também envolve as condições materiais para se informar, como poder pagar por veículos de informação, capacidade intelectual de buscar e de filtrar os conteúdos e a técnica para manusear as infraestruturas das plataformas comunicativas.<sup>10</sup> Um maior número de usuários na internet não implica em crescimento do capital informacional da população, pois não basta estar conectado à rede, é preciso preparo que decorre de processos educacionais\*.

\* Para saber mais, confira os conceitos de Letramento e Alfabetização digitais presentes no volume 1 deste glossário

### 1.3. Comunidade digital

A criação das comunidades digitais - ou ciber comunidades - faz parte da interação em rede. As tecnologias possibilitaram o aumento do fluxo de informação e de interação, uma vez que impulsionam o potencial comunicativo das ideias. Para Sillence e Baber<sup>11</sup>, comunidades digitais são grupos de pessoas que se engajam coletivamente sob algum domínio tecnológico, como a **web**. Diversos motivos servem como base para a formação de um grupo, entre eles: o reconhecimento de identidades afins; posicionamento e engajamento político; interesse comum por movimentos sociais, esportes, estudos ou por qualquer outra área.

Recentemente, o debate sobre a mescla das comunidades online e offline tem se fortalecido, no sentido de que organizações e movimentos sociais têm se utilizado da internet para conquistar engajamento que modifique o universo das coisas do “mundo offline”. Marcus Abílio Pereira (2001)<sup>12</sup>, discorre sobre como a internet serviu para oferecer novas estratégias de mobilização política, dando autonomia para que as pautas antes silenciadas sejam trazidas a público, além de permitir que grupos sociais adquiram visibilidade e criem uma imagem de si mesmos, diferentemente da dinâmica dos meios de comunicação tradicionais.



## 1.4. Atenção profunda / hiperatenção

Atenção profunda (em inglês, *deep attention*), é a capacidade de se concentrar unicamente em uma coisa, sem se deixar afetar por estímulos externos durante um longo período. Está em oposição à “hiperatenção”, entendida como a relação preferencial do indivíduo que muda frequentemente seu foco perante um denso fluxo informacional. Nela, os estímulos são constantes e os indivíduos têm a habilidade de lidar com muitas informações ao mesmo tempo. Em seu trabalho, Katherine Hayles descreve evidências da existência de um processo de transformação geracional em curso, com o predomínio do modo cognitivo da hiperatenção na vida das novas gerações.<sup>13</sup>

\* Rastros digitais são as informações registradas (nos servidores ou hardwares) a partir de ações realizadas pelo usuário ou processos automatizados na internet.

Certos rastros digitais são intencionais e outros são invisíveis e não-intencionais. Estes são informações secundárias a atividade principal do usuário. Por exemplo, quando o usuário solicita transporte privado por aplicativo o objetivo principal é o transporte. Entretanto, a plataforma armazena outras informações sobre o serviço, como a hora que a viagem começou e terminou

## 1.5. Clausura digital

Tradução livre do inglês *digital enclosure*. Andrejevic<sup>14</sup> descreve a clausura digital não somente como a partilha de um espaço digital, mas a característica de que toda informação das atividades online pode ser registrada e gerar um dado sobre ela mesma. Durante a utilização de tecnologias digitais na mediação de situações quotidianas, seja para realização de compras, pesquisas, uso de recursos de localização etc., geramos uma série de rastros digitais\* que permanecem armazenados e são utilizados para fins comerciais, por exemplo. Entre os possíveis usos comerciais dos rastros digitais, destaca-se o agrupamento dos dados para a formação de perfis comportamentais, técnica

denominada perfilamento, e utilização desses dados para direcionar publicidade de forma mais personalizada e persuasiva<sup>15</sup>.

## 1.6. Governo eletrônico

Em inglês o termo é encontrado como e-government. Diz respeito à incorporação de recursos das tecnologias da informação e comunicação (TICs) na Administração pública, modernizando a relação e a interação entre o governo, cidadãos, empresas e demais partes interessadas. Também envolve a ampliação do acesso e da possibilidade de participação, na medida em que órgãos governamentais passam a fornecer maior fluxo de serviços e informações por intermédio dos meios digitais, e maior integração das ferramentas da tecnologia da informação e comunicação (TICs) aos processos burocráticos e institucionais. No Brasil, por meio do Decreto de 3 de abril de 2000<sup>16</sup> o governo federal criou um Grupo de Trabalho Interministerial, com o objetivo de pensar o Programa de Governo Eletrônico do país. Segundo o site do e-Gov brasileiro, as diretrizes do sistema são construídas sobre três princípios: i) participação cidadã; ii) melhoria do gerenciamento interno do Estado; iii) integração com parceiros e fornecedores.<sup>17</sup> No entanto, o grupo de trabalho supracitado foi extinto pelo decreto Nº 10.087, de 5 novembro de 2019<sup>18</sup>. O uso das TIC(s) pelo governo no Brasil é também estudado pelo CETIC.br, que publica relatórios sobre governo eletrônico<sup>19</sup>.

## 1.7. Ética digital

Refere-se à prática de lidar com as possibilidades oferecidas pelo meio digital e suas tecnologias de forma responsável, combatendo a discriminação e todas as formas de preconceito e de exploração. Assuntos como privacidade, vigilância, robótica, segurança, propriedade intelectual, são temas comuns a essa discussão. Rafael Capurro escreve sobre o desenvolvimento da ética na rede e como isso pode contribuir para a superação dos desafios encontrados na era digital<sup>20</sup>.

## 1.8. Gerações tecnológicas

As gerações são marcadas pelo acesso tecnológico disponível característico de cada tempo. O conceito é explorado pelo campo de estudo sobre a relação entre recortes geracionais e a tecnologia. Sackmann e Weymann<sup>21</sup> trabalharam esse conceito ressaltando que as mudanças tecnológicas e sociais caminham em consonância e se modificam mutuamente. Por exemplo, a interação tecnológica de pessoas nascidas antes dos anos 1970 será muito diferente daquelas nascidos depois dos anos 2000. Também faz parte do estudo a observação sobre como a incorporação de tecnologias na vida cotidiana durante os anos de formação de uma pessoa influencia na forma como ela estará apta a acompanhar as mudanças tecnológicas subsequentes e a interagir com mundo digital na vida adulta.

## 1.9. Imersão digital

Conceito recorrentemente utilizado para se referir à experiência dos indivíduos com vídeo-games, como a possibilidade de inserção em outras narrativas, realidade aumentada, entre outras modalidades interativas que propiciam experiências de imersão. Além disso, o termo também se relaciona ao contato continuado de um indivíduo com a tecnologia.

Em um estudo sobre políticas públicas de Inclusão Digital, Echalar e Peixoto<sup>22</sup> apontam para a diferença entre fornecer o acesso pontual ao computador, seja na escola ou em **telecentros**, e a experiência contínua de tê-lo em casa e com acesso à internet. Segundo os autores, a experiência contínua seria a responsável por propiciar verdadeira imersão digital.

## 1.10. Imigrantes digitais

Autores como Marc Prensky<sup>23</sup> definem imigrantes digitais como aquelas pessoas que, diferentemente dos **nativos digitais**, não nasceram no chamado “mundo digital”, e que acabaram incorporando o uso das tecnologias digitais ao longo da vida.

No entanto, as distinções entre imigrantes e nativos digitais são apresentadas como relativas a um conflito entre gerações – nas quais a mais nova teria maior facilidade de aprendizagem com a tecnologia devido ao uso desde a infância, e a geração mais

antiga teria dificuldades pela inclusão das tecnologias digitais ao longo da vida. Essa questão é problematizada por diversos pesquisadores, como Monica Fantin, segundo a qual a aparente facilidade de jovens no uso de tecnologia não significa que eles tenham um uso consciente e crítico<sup>24</sup>.

### 1.11. Nativos digitais

A expressão nativos digitais tem como elemento central o tempo, uma vez que o critério para definir se um indivíduo é um nativo digital tem relação direta com a época de seu nascimento. Considera-se nativo digital aquele que nasceu a partir da década de 90, início da comercialização da internet<sup>25</sup>, cujas atividades cotidianas, desde os primeiros anos de vida, envolvem processos que perpassam, direta ou indiretamente, o uso da internet.

“Digital” pode ser definido como o adjetivo utilizado para “dispositivo que opera com valores binários exclusivamente”<sup>26</sup>. A linguagem utilizada na internet baseia-se em valores binários e, a partir de sua popularização, os indivíduos e grupos sociais puderam interagir com dispositivos conectados à rede. Assim, foi ampliado o contato da população com o mundo digital. Essa utilização por parte dos nativos digitais é amplificada aos diferentes espectros existenciais, ampliando o impacto das novas tecnologias se comparado às gerações anteriores.

Conforme afirmado por Prensky, o grande

volume de interação com a tecnologia altera os modelos de pensamento dos indivíduos. Consequentemente, diferentes dimensões da vida coletiva e individual também são manifestadas de formas distintas. Destaca-se a diferença na “formação da identidade entre as gerações pré-digitais, no sentido de que há mais experimentação e reinvenção das identidades, e diferentes modos de expressão, como o YouTube e os blogs”<sup>27</sup>.

Entretanto, uma análise unilateral e acrítica pode incorrer na ideologização da tecnologia, considerando-a panaceia e produtora do humano, em vez de produto do ser<sup>28</sup>. Portanto, a análise do cenário em sua totalidade considera dois níveis de nativos digitais: aqueles que desde a primeira infância têm acesso às tecnologias a partir da posse e frequência do acesso, e aqueles que utilizam as tecnologias aplicando habilidades e competências digitais desenvolvidas em outras fases da vida<sup>29</sup>.

\* Ver definição de digital, no conceito "Nativos Digitais" da seção Sociedade da Informação

## 1.12. Plataformas digitais\*

Originária das teorias econômicas de mercados bilaterais<sup>30</sup>, que pressupõem dois tipos de clientes que dependem um do outro para a plena consecução do negócio, as plataformas digitais são modelos de negócios “que utilizam a tecnologia com o intuito de conectar pessoas e promover interações”<sup>31</sup>.

O principal capital dessas plataformas é a informação, uma vez que as interações entre usuários aumentam o conhecimento

que a plataforma tem de seus usuários. Esse conhecimento, por sua vez, é maximizado proporcionalmente ao volume de dados tratados<sup>32</sup>.

Gawer e Cusumano abordam o conceito amplo de plataforma e as dividem em duas formas predominantes: internas e externas. As plataformas internas são um conjunto de ativos organizados a partir de uma estrutura comum da instituição, que servem para o próprio empreendimento desenvolver produtos derivados. Um exemplo de plataforma digital interna seria o conjunto de ativos (ferramentas de balanço de caixa, contagem de estoque, atendimento ao cliente) que uma empresa de e-commerce possui para conseguir vender seus produtos virtualmente<sup>33</sup>. Já as plataformas externas são produtos, serviços ou tecnologias que fornecem a base sobre a qual outras instituições que não a proprietária da plataforma podem desenvolver seus próprios produtos, tecnologias ou serviços complementares. O motor de busca da Google é um exemplo de plataforma digital externa, uma vez que é um conjunto de tecnologias que organiza a informação disponibilizada na internet<sup>34</sup>.

As plataformas digitais com altos faturamentos, como Google, Apple, Facebook e Amazon (GAFA), utilizam dados informados pelos usuários durante a navegação como insumo de seu modelo de negócio. A disponibilidade de um colossal volume de dados nos sistemas de armazenamento das plataformas digitais é justificada pela

dualidade fundamental das tecnologias da informação e comunicação (**TICs**), conforme aponta Shoshana Zuboff<sup>35</sup>. Ou seja, as TICs são utilizadas para automatizar operações e facilitar o trabalho do indivíduo e impõem informações ao sistemas que irá utilizar. Simultaneamente, a automação gera informações, em torno das quais são organizados os modelos de negócio de plataformas aparentemente gratuitas. Esse fenômeno de intensa produção e disponibilização de dados que baliza a afirmação e crescimento das plataformas digitais no mercado é chamado de big data.

### 1.13. Privacidade

Trata-se de um conceito sobre o qual não há consenso e que tampouco está redigido objetivamente na lei, o que traz problemas para a sua aplicação, como argumentado por Marcel Leonardi<sup>36</sup>. Há uma gama de expressões que são utilizadas para se referir à privacidade, tais como segredo, intimidade, e mesmo a Constituição Federal de 1988 não cita a palavra privacidade, mas sim declara inviolável o direito “à vida privada”<sup>37</sup>. Isso significa que a Constituição elegeu esse direito como dotado de uma proteção especial por parte do Estado brasileiro. Sendo assim, o indivíduo ou a coletividade, frente a uma violação da privacidade, possuem o poder de exigir reparações e respostas do Estado, bem como do setor privado, pela violação<sup>38</sup>.

Em uma contextualização mais prática e histórica, Marcel Leonardi aponta que os conceitos unitários de direito à privacidade



podem ser divididos em 4 principais categorias<sup>39</sup>:

1. **Direito de ser deixado só**<sup>40</sup>, que está na “paz de espírito ou no alívio assegurado pela capacidade de impedir a própria publicação”;
2. **Resguardo contra interferências alheias**, que abrange a ideia de intimidade de um indivíduo, o qual possui o direito de escolher o que pode ou não ser publicizado;
3. **Segredo ou sigilo**, que se baseia na divisão entre informações públicas e privadas e entende a violação do direito à privacidade como a publicização de uma informação privada;
4. **Controle sobre informações e dados pessoais**, que entende a privacidade não como a ocultação de informações privadas, mas sim como a autonomia dos indivíduos no controle sobre seus dados pessoais.

Danilo Doneda argumenta que a compreensão da privacidade sofreu mudanças nas últimas décadas, se deslocando de uma percepção individualista do conceito para uma dimensão coletiva. A proteção da privacidade na era da informação se atenta à garantia do sujeito de estabelecer sua vida privada e de deliberar positivamente sobre ela em suas relações sociais<sup>41</sup>. Segundo o autor, na contemporaneidade, uma das

formas com as quais o direito à privacidade se manifesta é por meio da proteção dos dados pessoais, administrando os interesses relacionados à personalidade e às liberdades pessoais em relação à dinâmica social<sup>42</sup>

Desse modo, a compreensão e aplicação desse direito perpassa diferentes contextos sociopolíticos e jurisdições e, por isso, a privacidade se apresenta como um conceito de definição variável. Em linhas gerais, o direito à privacidade se relaciona diretamente ao desenvolvimento da personalidade e à democracia, baseando-se na dicotomia entre as esferas pública e privada<sup>43</sup>. Bruno Bioni aponta que, partindo do pressuposto de que o desenvolvimento da subjetividade dos indivíduos perante a sociedade acontece principalmente no âmbito privado, longe da pressão social, considera-se a privacidade um direito estático e que opera na lógica de liberdade negativa. Entende-se o conceito como um direito estático, pois se relaciona ao dever do indivíduo de delimitar o que deve ou não ser compartilhado em âmbito público; enquanto o exercício de uma liberdade negativa de um indivíduo está atrelado à ideia “não sofrer interferência alheia”<sup>44</sup>.

Na doutrina internacional, Kuner, Cate e coautores dissertam sobre a complexidade do termo<sup>45</sup> e apresentam tensões emergentes para sua compreensão na contemporaneidade. Entre elas estão a tensão entre privacidade como um direito e privacidade como um produto, pois, apesar de estar garantida em normas, a privacidade tem sido frequentemente apropriada para

a atribuição de um valor comercial. Isso gera conflitos para a maioria dos sistemas jurídicos que têm dificuldade de entender o caráter bivalente do tratamento de dados pessoais atrelado à privacidade. Ocorre, também, a tensão entre privacidade e interesses governamentais, na medida em que historicamente os governos têm interesse em conhecer e registrar dados da população a partir de pesquisas, ainda que isso seja regulado em muitos países nos últimos anos. Há a tensão entre privacidade e segurança, que costuma reforçar a figura do estado na administração dos dados, ao passo que é a figura institucional responsável pela segurança pública. No entanto, não é evidente o entendimento de quais dados são necessários para a manutenção da segurança geral e esses conceitos não podem ser compreendidos como auto excludentes, mas equilibrados caso a caso. Os autores pontuam que apesar da sua natureza complexa, a maioria dos estados concordam que a privacidade se trata de um domínio sobre o qual deve haver um esforço de proteção e regulação, e compreendem que há um entendimento básico sobre a privacidade como direito sobre a qual se deve zelar.

Solove<sup>46</sup> ressalta que com frequência são adotadas concepções limitadas sobre privacidade, restringindo a sua violação por divulgação de dados pessoais ou pelo atentado ao segredo. Contudo, essa abordagem no âmbito jurídico pode dificultar o entendimento do que seria uma violação e, assim, não efetivar o conceito como direito. Para o autor, privacidade

tem a ver com o respeito aos desejos dos indivíduos assegurado por normas. É, também, um direito coletivo, pois assegura um espaço privado importante para a liberdade e bem estar dos sujeitos. Solove apresenta uma taxonomia da privacidade, localizando situações em que ela pode ser um problema em quatro grupos diferentes: coleta, processamento, disseminação da informação, e casos de invasão. Compreendidas nessas categorias estão as atividades que apresentam problemas para a privacidade, tais como vigilância, identificação, exposição, exclusão, uso de dados para outros fins, distorção de informação, entre outras.

Por fim, Zittrain<sup>47</sup> escreve sobre privacidade na era da **web 2.0** e discute sobre a mescla da vida pública e privada na forma como nos colocamos e nos expomos internet. O autor sustenta que a ideia de privacidade nos leva a admitir a existência de um lugar privado, um “locus” onde possamos resguardar artefatos, memórias, histórias e outros elementos que constituem a nossa identidade sem que haja interferência ou interrupção.

## 1.14. Proteção de dados

Conjunto de medidas que buscam garantir o direito à privacidade, com o objetivo de conferir ao indivíduo autonomia sobre o controle de seus dados pessoais<sup>48</sup>. Apesar de estar relacionado ao direito à privacidade, a proteção de dados pessoais com ele não se confunde, pois se baseia

não na dicotomia entre os âmbitos público e privado, mas sim no conceito de dados pessoais - que podem estar presentes tanto na esfera pública quanto privada. De acordo com Bruno Bioni, o direito à proteção de dados pessoais é dinâmico, na medida em que é construída por meio do controle e tratamento<sup>49</sup> de dados pessoais.

A compreensão que vigora sobre dados pessoais denota dados relativos à pessoa natural identificada ou identificável. Políticas legislativas e regulatórias sobre essa matéria, como a Convenção 108 do Conselho Europeu<sup>50</sup> e o Regulamento Geral de Proteção de Dados da União Europeia<sup>51</sup> são exemplos de conjuntos de medidas que buscam disciplinar o tratamento, isto é, uma série de operações que têm por objeto dados pessoais, por agentes públicos e privados<sup>52</sup>.

A proteção de dados também está relacionada à noção de autodeterminação informacional, uma vez que o indivíduo tem o direito de consentir o uso de seus dados. No entanto, também é importante salientar que existem interesses de diversas naturezas no fluxo e tratamento de dados pessoais que afetam diretamente os direitos e desenvolvimento da personalidade dos indivíduos<sup>53</sup>.

Um exemplo de mecanismo legal é a Lei Geral de Proteção de Dados Pessoais (LGPD), que

Dispõe sobre o tratamento  
de dados pessoais,

inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.<sup>54</sup>

### 1.15. Provedor de internet

Os provedores são empresas responsáveis por intermediar as atividades de usuários na internet. Marcel Leonardi aponta que, entre os diversos tipos de provedores, “provedor de serviços de internet” é a expressão utilizada para se referir a toda “pessoa natural ou jurídica que fornece serviços relacionados ao funcionamento da internet, ou por meio dela”<sup>55</sup>. A categoria provedor de serviços de internet abarca diversos tipos de provedores, de acordo com a natureza da atividade que desempenham.

O Marco Civil da Internet<sup>56</sup> traz previsões legais que incidem sobre dois tipos de provedores: os provedores de conexão e os provedores de conteúdo. A lei não conceitua diretamente os tipos de provedores, mas sim o que se considera “conexão” ou “aplicações de internet”<sup>57</sup>. O provedor de conexão - ou ainda, acesso - é a empresa responsável por prover conexão de dispositivos à rede que permite que os usuários acessem a internet.

No Brasil algumas das empresas mais conhecidas são NET Virtua, GVT, Oi, Vivo, Sky, entre outras. Já os provedores de aplicação são aqueles que provem “o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet”<sup>58</sup>, ou seja, plataformas como Youtube e Facebook. Na prática, é comum que a mesma empresa que provê a conexão também seja uma provedora de aplicação, o que resulta em certas confusões conceituais, embora a natureza das atividades não se confundam. A exemplo a empresa NET, que oferece serviço de conexão, mas também dispõe de uma plataforma de serviços de streaming (aplicação), como é conhecido o serviço de transmissão online.

## 1.16. Mídias sociais

Segundo Andreas Kaplan e Michael Haenlein, mídias sociais - ou ainda, em inglês, *social media* - são um grupo de aplicações de internet que permite troca de conteúdos criados por seus usuários no contexto da web 2.0<sup>59</sup>.

Os autores propõem uma categorização das mídias sociais considerando o nível de presença social, isto é, as formas de contato que uma mídia possibilita entre seus usuários, e também de autoapresentação, que está relacionada à possibilidade de o usuário construir sua própria imagem online. Blogs, redes sociais, projetos colaborativos como a Wikipedia e jogos online seriam todos mídias sociais, mas com níveis de presença social e autoapresentação distintos.

## 1.17. Sociedade digital

Característica de sociedades contemporâneas nas quais processos de interação, socialização, aprendizagem e partilha acontecem de forma expressiva no meio digital. Nessa realidade, o conhecimento se organiza em rede, e as fronteiras entre os espaços de aprendizagem se diluem nas plataformas online<sup>60</sup>, que funcionam potencialmente como espaço de troca, informação, expressão, trabalho e convívio.

## 1.18. TIC

TIC é a sigla utilizada para se referir às tecnologias da informação e comunicação largamente incorporadas ao cotidiano da sociedade da informação. Relaciona-se com o uso das ferramentas da tecnologia na troca, criação e busca por informações.

No Brasil, em 2015, foi criado o Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br)<sup>61</sup>, órgão responsável pelo monitoramento do uso das TICs (em especial, o acesso e uso de computador, internet e dispositivos móveis) nos contextos brasileiros. O Cetic.br publica pesquisas sobre a disponibilidade e uso das TICs na educação, na cultura, nos domicílios, na área da saúde, por crianças e adolescentes, governo, empresas, organizações sem fins lucrativos (OSFIL), entre outras.



## 1.19. Telecentro

Espaço público que oferece acesso a computadores e internet para a comunidade em geral. Frequentemente, cursos e capacitações são ofertados nesses espaços a partir de parcerias, para promover ações de inclusão digital.

## 1.20. Tecropolítica

Essa definição, assim como as outras presentes neste glossário, não tem como objetivo esgotar a discussão sobre um tema tão dinâmico. Os estudos sobre tecropolítica têm versado sobre a relação entre tecnologias da informação e política, especialmente sobre o potencial transformador que uma esfera exerce sobre a outra. Nesse contexto, a internet é construída e modificada de forma constante pelos indivíduos que a compõem. As questões vivenciadas em sociedade são sistematicamente projetadas nas redes, o que traz novos desafios políticos e questões regulatórias sobre um espaço que se consolidou na dinâmica social há relativamente pouco tempo e que se transforma a cada dia.

Winner<sup>62</sup> nos adverte, em 1980, sobre o perigo de se acreditar em um “determinismo tecnológico”, no sentido de que as tecnologias se desenvolvem a partir de suas próprias métricas e dinâmicas, e, então, passariam a transformar a sociedade. Entretanto, todo desenvolvimento tecnológico acontece contextualizado em realidades sociais e

econômicas, que se modificam mutuamente. O autor também exemplifica como formas e infraestruturas tecnológicas têm inferências políticas práticas, como a possibilidade ou não de interação e de inclusão de determinados grupos minoritários, como as pessoas com deficiência.

Gagliardone<sup>63</sup> destaca quatro contribuições que os estudos em tecnopolítica oferecem para a compreensão dos fenômenos sociais. A primeira contribuição envolve a diferença na forma como estados e organizações implementam e usufruem de uma tecnologia de acordo com o contexto (a exemplo, países que controlam o conteúdo disponibilizado na internet, como a China, onde o ecossistema da internet é controlado pelo governo e alguns sites têm o acesso bloqueado ou parte do conteúdo é banido). A segunda contribuição se relaciona à influência que a política exerce sobre a infraestrutura e a forma das tecnologias, incluindo, por exemplo, as ideologias dos atores envolvidos nos processos que moldam os avanços e a construção da própria tecnologia. A terceira delas refere-se ao poder: artefatos tecnológicos podem servir como forma de exercício de poder, ao passo que permitem que se estabeleça e exerça autoridade. Por fim, tecnopolítica também inclui a posição de destaque dos governos nesse contexto, sendo, em muitos dos casos, a entidade com maior concentração de recurso e poder para intervir na formação da tecnologia, entender como os diferentes atores se valem dela e construir elementos discursivos e materiais com os quais lidará

em prol de suas aspirações políticas.

## 1.21. Transculturalidade

Ao escrever sobre transculturalidade, Welsch<sup>64</sup> aponta duas instâncias: macro e micro. A perspectiva macro compreende a partilha e mescla de modos de vida e de cultura pelos povos de um mesmo território, fazendo emergir um contexto em que múltiplas culturas se somam e atravessam a vida das pessoas de forma constitutiva. Em uma perspectiva mais focalizada (micro), transculturalidade evidencia as múltiplas categorias definidoras que compõem a identidade de um indivíduo, desde nacionalidade e idioma, até recortes de classe e de gênero. O autor ressalta que, ao contrário do que se poderia pensar, a transculturalidade não é um fenômeno homogeneizante, mas uma possibilidade de ampliação do espectro de diversidade com o qual os indivíduos interagem que favorece a coexistência em vez do combate.

Em razão de sua natureza e do funcionamento independente de localização geográfica, a internet se constitui como um ambiente sem fronteiras. Nela, múltiplas culturas estão em relação e em possibilidade de troca e conexão, favorecendo, idealmente, a consolidação de uma cultura diversa e transcultural.

## 1.22. Web 2.0

Sobre a internet se constituiu uma interface de compartilhamento de informações e serviços que modificou e potencializou as possibilidades de interação entre indivíduos, consolidando a denominada Web 2.0. Essa mudança é entendida como uma nova etapa da tecnologia, que inaugurou novidades importantes para a compreensão da dinâmica social, alterando as formas das trocas informacionais e comunicacionais, interações pessoais e tendências mercadológicas<sup>65</sup>.

Tim O'Reilly ressalta como a principal característica da Web 2.0 a possibilidade de criação de aplicativos e plataformas que se aproveitem do que ele chama “inteligência coletiva”, quando a tecnologia se aprimora na medida em que mais pessoas a utilizam<sup>66</sup>. Enquanto que a internet 1.0 era marcada pela baixa interatividade entre os usuários, que eram numericamente bem menores do que o de hoje em dia. O conteúdo era exclusivamente aquele criado pelos donos dos sites, sem espaço para a interação.

## 1.23. Moderação de conteúdo

Grande parte do conteúdo disponível na internet é veiculado em **plataformas digitais** de empresas privadas, destacando-se as plataformas de busca, redes sociais e outros intermediários<sup>67</sup>. Por meio de políticas e termos de uso, são estabelecidas regras sobre quais são os conteúdos que podem ser

veiculados nas interfaces das plataformas e quais serão bloqueados ou excluídos. A atuação de empresas, governos ou outros atores na determinação dos conteúdos que permanecem ou são retirados em suas ferramentas é chamada moderação de conteúdo. Percebe-se, na prática, grande concentração de poder, por entes privados, sobre a liberdade de expressão dos usuários dos serviços que fornecem.

A moderação de conteúdo pode ser realizada por meio de inteligência artificial ou por funcionários das plataformas. Entre os tipos de moderação, destacam-se os filtros de conteúdo que impedem o upload de determinadas informações e a análise de publicações denunciadas por usuários da rede por desrespeito às regras da plataforma. Por exemplo, um vídeo que contém pornografia ou conteúdo sexual explícito poderá ser removido do Youtube, pois esse tipo de conteúdo não é aceito pelas diretrizes da comunidade do Youtube<sup>68</sup>.

Com objetivo de assegurar que os padrões das plataformas digitais estejam de acordo com direitos humanos, diversos atores direcionam esforços para a construção de modelos de regulação dos limites e modos de atuação dessas plataformas. A moderação de conteúdo desperta especial preocupação em relação à liberdade de expressão e de pensamento, bem como proteção contra censura e discriminação, uma vez que se reflete em uma decisão sobre o conteúdo que circula na camada de conteúdo da internet.

A regulação dos meios de comunicação é prática adotada em diversos países como Canadá<sup>69</sup> e Austrália<sup>70\*</sup>. Entre os argumentos que legitimam a regulamentação estatal, destaca-se a consideração de que o setor das telecomunicações possui grande poder sobre a construção do pensamento coletivo e identidade dos indivíduos. A relação entre o setor das telecomunicações e internet é estabelecida uma vez que todo o tráfego de dados que compõem a internet é realizado por meio da infraestrutura das telecomunicações<sup>71</sup>. Entretanto, os tradicionais sistemas de telecomunicações, como a telefonia fixa e a televisão por assinatura, não possuem as peculiaridades próprias da internet.

Por ser uma rede baseada na coleta, armazenamento, processamento e comunicação de dados<sup>72</sup>, a quantidade de informações e de interações entre os usuários na internet é bastante volumosa. Além disso, as características técnicas da internet, como a comunicação fim-a-fim e o cabeamento transoceânico, exigem que a regulação das comunicações na rede sejam elaboradas de acordo com essas especificidades. Entre as propostas para o estabelecimento de critérios para veiculação de conteúdo veiculado na internet, destacam-se a proposta elaborada por organizações da sociedade civil latino-americanas intitulada “Contribuições para uma regulação democrática das grandes plataformas que garanta a liberdade de expressão na internet”<sup>73</sup>. No setor privado, observa-se a construção do “Conselho Externo de Supervisão” das decisões do

\* A Comissão Canadense de Rádio-Televisão e Telecomunicações promulgou diversos regulamentos que incidem diretamente sobre o conteúdo disponibilizado pelos meios de comunicação. Por exemplo, a Comissão impede que emissoras de TV transmita comentários que expressem desprezo por um grupo ou indivíduo, além de regulamentar sobre publicidade comercial e o material eleitoral político partidário. Recentemente, a Austrália aprovou uma emenda ao Código Penal para exigir que plataformas digitais removam rapidamente conteúdos de exposição de sequestros, assassinatos, estupro ou ataques terroristas sob pena de prisão dos funcionários da plataforma e pagamento de multa.

\* 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. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, Disponível em: <<https://bit.ly/1kxaoKm>>. Acesso em: 22 set. 2019.

## Facebook sobre conteúdos controversos na plataforma<sup>74</sup>.

Até o momento, o governo brasileiro não possui legislação ou projetos de lei nessa temática em específico. A Lei nº 12.965, de 23 de abril de 2014, Marco Civil da internet, é o principal instrumento legal que dispõe sobre a responsabilização dos **provedores** de conteúdo por conteúdos publicados por usuários das plataformas. De acordo com a legislação brasileira, os provedores de conteúdo não são obrigados a fiscalizar ou a moderar o conteúdo publicado pelos usuários da plataforma<sup>75\*</sup>.

## NOTAS

- 1 ROGERS, Everett. **Informatization, globalization, and privatization in the new Millenium**. Asian Journal of Communication, v. 10, n. 2, p. 71-92, 2000. Disponível em <<https://bit.ly/2kGTQJx>>. Acesso em 12 set. 2019.
  
- 2 Tradução livre de: “In an information society, information is the vital ingredient, as energy was in the industrial society and as manual labour was in the agricultural”. ROGERS, Everett. **Informatization, globalization, and privatization in the new Millenium**. Asian Journal of Communication, v. 10, n. 2, p.73. Disponível em <<https://bit.ly/2kGTQJx>>. Acesso em 12 set. 2019.
  
- 3 CASTELLS, Manuel. **A era da informação: economia, sociedade e cultura**. In: A Sociedade em rede. São Paulo : Paz e Terra, 2000. v. 1. p. 107 a 118.
  
- 4 BRAGA, Julião et al. **O livro do IETF. CGI. br**, São Paulo, v. 1, 2014. Disponível em <<https://bit.ly/2kviJlh>>. Acesso em 20 set. 2019
  
- 5 CGI.BR. **Documentos da Cúpula Mundial sobre a Sociedade da Informação**. CGI. br, São Paulo, v. 1, 2014. Disponível em <<https://bit.ly/2Yh1TtM>>. Acesso em 20 set. 2019.
  
- 6 KURBALLJA, Jovan. **Uma introdução à governança da internet**. São Paulo: Comitê Gestor da Internet no Brasil, 2016. Disponível em <<https://bit.ly/2w8OQ2r>>. Acesso em 20 set. 2019
  
- 7 CGI.br. **Sobre o CGI.br**. Disponível em <<https://bit.ly/2m7IazU>>. Acesso em 23 set. 2019
  
- 8 BRASIL. **Portaria Interministerial nº 147, de 31 de maio de 1995**. Brasília, 31 maio 1995. Disponível em: <<https://bit.ly/2kRiYOp>>. Acesso em: 23 set. 2019.
  
- 9 CGI.BR. **Resolução CGI.br/RES/2009/003/P**. Disponível em <<https://bit.ly/2m74biq>>. Acesso em 23 set. 2019.
  
- 10 HAMELINK, Cees J. **The ethics of cyberspace**. Sage, 2000. Disponível em <<https://bit.ly/2m95U6B>>. Acesso em 12 set. 2019.
  
- 11 SILENCE, Elizabeth; BABER, Chris. **Integrated digital communities: combining web-based interaction with text messaging to develop a system for encouraging group communication and competition**. Interacting with computers, v. 16, n. 1, p. 93-113, 2004. Disponível em <<https://bit.ly/2IKTsKn>>. Acesso em 12 set. 2019.
  
- 12 PEREIRA, Marcus Abílio. **Internet e mobilização política - os movimentos sociais na era digital**. In: IV Encontro da Compolitica, 2011, Rio de Janeiro. Anais do IV Encontro da Associação Brasileira de Pesquisadores em Comunicação e Política, 2011. p. 1 - 26. Disponível em: <<http://bit.ly/35BKv8b>>. Acesso em: 28 out. 2019.



- 13 HAYLES, N. Katherine. **Hyper and deep attention**: The generational divide in cognitive modes. *Profession*, v. 2007, n. 1, p. 187-199, 2007. Disponível em <<https://bit.ly/2ELiGA9>>. Acesso em 09 set. 2019.
- 14 ANDREJEVIC, Mark. **Privacy, exploitation, and the digital enclosure**. *Amsterdam LF*, v. 1, p. 47, 2008. Disponível em <<https://bit.ly/2m6QcsG>>. Acesso em 12 set. 2019.
- 15 DE CASTRO, Julio Cesar Lemes. **O consumo na era da interpelação algorítmica**. Disponível em <<https://bit.ly/2pnqnXp>>. Acesso em 20 out. 2019
- 16 BRASIL. **Decreto de 03 de abril de 2000**. Institui Grupo de Trabalho Interministerial para examinar e propor políticas, diretrizes e normas relacionadas com as novas formas eletrônicas de interação. Brasília, Disponível em: <<https://bit.ly/2OsU55t>>. Acesso em: 12 set. 2019.
- 17 Ministério da Economia. **Governo Eletrônico**. Disponível em: <<https://bit.ly/2khUhdD>>. Acesso em: 12 set. 2019.
- 18 BRASIL. **Decreto Nº 10.087, de 5 de novembro De 2019**. Declara a revogação, para os fins do disposto no **art. 16 da Lei Complementar nº 95, de 26 de fevereiro de 1998**, de decretos normativos. Brasília, Disponível em: <<http://bit.ly/2EwX0WC>>. Acesso em: 13 nov. 2019.
- 19 CETIC.br. **Pesquisa sobre o uso das Tecnologias de Informação e Comunicação - TIC Governo Eletrônico 2017**. Disponível em <<http://bit.ly/2PAHKy9>>, acesso em 28 out. 2019.
- 20 CAPURRO, Rafael. **Digital Ethics**. Disponível em: <<https://bit.ly/2lOMzaI>>. Acesso em: 12 set. 2019.
- 21 SACKMANN, Reinhold; WEYMANN, Ansgar. **Die technisierung des alltags**: Generationen und technische innovationen. Campus-Verlag, 1994. Disponível em <<https://bit.ly/2kjE4Eo>>. Acesso em 09 jul. 2019.
- 22 ECHALAR, Adda Daniela Lima Figueiredo; PEIXOTO, Joana. **Programa Um Computador por Aluno**: o acesso às tecnologias digitais como estratégia para a redução das desigualdades sociais. Ensaio: Avaliação e Políticas Públicas em Educação, v. 25, n. 95, p. 393-413, 2017. Disponível em ECHALAR, PEIXOTO - Programa um computador por aluno: o acesso às tecnologias digitais como estratégia para a redução das desigualdades sociais. Disponível em <<https://bit.ly/2lSWV9q>>. Acesso em 03 jul. 2019.
- 23 PRENSKY, Marc. **Digital Natives, Digital Immigrants**. On the Horizon, Vol. 9 No. 5, NCB University Press, 2001. Disponível em: <<https://bit.ly/2ySL1ib>>. Acesso em: 1 ago. 2019.
- 24 FANTIN, Monica. **“Nativos e imigrantes digitais” em questão**: crianças e competências midiáticas na escola. p.9. Passagens, Ceará, 2016. Disponível em: <<http://bit.ly/2EsHYkC>>. Acesso em: 1 ago. 2019.

- 25 TERRA. **Anos 90:** o desenvolvimento da internet no Brasil. Disponível em: <<https://bit.ly/2IRIUZE>>. Acesso em: 12 set. 2019.
- 26 MICHAELIS. **Digital.** Disponível em: <<https://bit.ly/2kxxTg8>>. Acesso em: 12 set. 2019.
- 27 PALFREY, John; GASSER, Urs. **Nascidos na era digital:** entendendo a primeira geração de nativos digitais. Penso Editora, 2011. p. 31. Disponível em <<https://bit.ly/2kJKGvI>>. Acesso em 1 set. 2019
- 28 LOUREIRO, Carla Cristiane; GRIMM, Viviane; LUNARDI-MENDES, Geovana M. **“imigrantes” versus “nativos” digitais:** O discurso de tecnologias digitais em políticas curriculares. Roteiro, v. 41, n. 3, p. 731, 2016. Disponível em <<https://bit.ly/2lMufz4>>
- 29 PONTE, Cristina; SIMÕES, José Alberto. **Comparando resultados sobre acessos e usos da internet:** Brasil, Portugal e Europa. Comitê Gestor da Internet no Brasil-CGI. BR. TIC Kids Online Brasil, p. 27-35, 2012.
- 30 SALTARELLI, Bia. **Plataformas digitais:** o que é e como as grandes empresas do mundo utilizam? Disponível em: <<https://bit.ly/2kxyj28>>. Acesso em: 12 set. 2019.
- 31 Ibid.
- 32 De acordo com a nova Lei Geral de Tratamento de Dados Pessoais (LGPD), tratamento de dados é “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 14 ago. 2018. Disponível em: <<https://bit.ly/2LIYwGr>>. Acesso em: 23 set. 2019.
- 33 PASCOTTO, Alan. **Quais são os tipos de plataforma de e-commerce?.** Disponível em <<https://bit.ly/2m9Gmq3>>. Acesso em 23 set. 2019.
- 34 GAWER, Annabelle; CUSUMANO, Michael A. Industry platforms and ecosystem innovation. **Journal of product innovation management**, v. 31, n. 3, p. 417-433, 2014. Disponível em <<https://bit.ly/2kevcXj>>. Acesso em 11 set. 2019.
- 35 ZUBOFF, S. **Big other:** Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, v.30, n.1. p. 75-89. 2015.
- 36 LEONARDI, Marcel. **Tutela e privacidade na internet.** São Paulo: Saraiva, 2011.
- 37 Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas,

assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil de 05 de outubro de 1988. Brasília, Disponível em: <<https://bit.ly/1bJYIGL>>. Acesso em: 12 set. 2019.

38 VIEIRA, Victor B. R.; CORASSA, Eugênio D. **A importância da proteção de dados pessoais como direito fundamental**. Disponível em <<https://bit.ly/2kjlICk>>. Acesso em set. 2019.

39 LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2011.

40 WARREN, Samuel D.; BRANDEIS, Louis D. **The right to privacy**, in 4 Harvard Law Review 193, 1890.

41 DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais**. Rio de Janeiro: Renovar, 2006. p.24.

42 Ibidem, p. 30.

43 BIONI, Bruno. **Proteção de dados pessoais: A função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. p. 94.

44 Idem. p. 96

45 KUNER, C., CATE, F. H., MILLARD, C., e SVANTESSON, D. J. B. **Privacy—an elusive concept**. International Data Privacy Law, 1(3), 2011. p. 141-142.

46 SOLOVE, Daniel. **Understanding privacy**. Harvard University Press, 2010.

47 ZITTRAIN, Jonathan. **Privacy 2.0**. University of Chicago Legal Forum. 2008. Pag 65. Disponível em <<http://bit.ly/2sFwHuC>>. Acesso em 11 dez. 2019.

48 IRIS. **Representação ao Ministério Público de Minas Gerais - MPMG. 2018**. Disponível em: <<http://bit.ly/32Z4cp1>>. Acesso em 29 out. 2019.

49 Segundo o decreto que regulamenta o Marco Civil da internet, o tratamento de dados pessoais consiste em “[...] toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”. BRASIL. **Decreto nº 8.771, de 11 de maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Brasília, Disponível em: <<http://bit.ly/38TVUSQ>>. Acesso em: 22 out. 2019.

50 CONSELHO EUROPEU. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. Estrasburgo, 1981. Disponível em: <<http://bit.ly/2EwEJsE>>. Acesso em: 20 nov. 2019.

51 UNIÃO EUROPEIA. **Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, Estrasburgo, 04/05/2016. Disponível em: <<https://bit.ly/2S2WGH7>>. Acesso em: 20 nov. 2019.

52 POLIDO, Fabrício, et al. **GDPR e suas repercussões no direito brasileiro**: primeiras impressões de análise comparativa. Instituto de Referência em Internet e Sociedade: Belo Horizonte, 208. Disponível em: <<https://bit.ly/2BEcG8W>>. Acesso em: 23 de out. de 2019.

53 BIONI, Bruno. **Proteção de dados pessoais**: A função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 25.

54 BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, Disponível em: <<https://bit.ly/2LIYwGr>>. Acesso em: 10 set. 2019.

55 LEONARDI, Marcel. **Responsabilidade Civil dos Provedores de Serviços de Internet**. Disponível em: <<https://bit.ly/2kkOMKO>>. Acesso em 06 set. 2019.

56 BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, Disponível em: <<https://bit.ly/1kxaoKm>>. Acesso em: 10 set. 2019.

57 Art. 5º Para os efeitos desta Lei, considera-se: I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes; II - terminal: o computador ou qualquer dispositivo que se conecte à internet; III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais; IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País; V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP; VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados; VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP. BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, Disponível em: <<https://bit.ly/1kxaoKm>>. Acesso em: 10 set. 2019.

- 58 BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Art 5º. Brasília, Disponível em: <<https://bit.ly/1kxaoKm>>. Acesso em: 10 set. 2019.
- 59 KAPLAN, Andreas M. HAENLEIN, Michael. **Users of the world, unite!** The challenges and opportunities of Social Media. Business Horizons, Estados Unidos, 53, p.59-68, 2010. Disponível em: <<https://bit.ly/2YWtNwU>>. Acesso em 06 set. 2019.
- 60 DIAS, Paulo. **Comunidades de educação e inovação na sociedade digital.** Educação, Formação & Tecnologias-ISSN 1646-933X, v. 5, n. 2, p. 4-10, 2012. Disponível em <<https://bit.ly/2kzafjm>>. Acesso em 13 set. 2019.
- 61 Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação Cetic.br. Disponível em <<https://bit.ly/2maNouB>>. Acesso em 26/08/2019.
- 62 WINNER, Langdon. **Do artifacts have politics?**. Daedalus, p. 121-136, 1980. Disponível em <<https://bit.ly/2TuKEXZ>>, acesso em 19/08/2019.
- 63 GAGLIARDONE, Iginio. **"A country in order"**: Technopolitics, nation building, and the development of ICT in Ethiopia. Information Technologies & International Development, v. 10, n. 1, p. pp. 3-19, 2014. Disponível em <<https://bit.ly/2m9qBzl>>. Acesso em 13 set. 2019
- 64 WELSCH, Wolfgang. **Transculturality**: The puzzling form of cultures today. Spaces of culture: City, nation, world, v.13, n. 7, p. 194-213, 1999. Disponível em <<https://bit.ly/2m9qMdZ>>. Acesso em 23 ago. 2019.
- 65 PRIMO, A. **O aspecto relacional das interações na Web 2.0.** E-Compós, Brasília, v.9, p.1-21, 2007. Disponível em <<https://bit.ly/2m8y29Y>>. Acesso em 13 set. 2019.
- 66 O'REILLY, Tim. **Web 2.0 Compact Definition**: Trying Again. Disponível em <<https://bit.ly/NIA49S>>. Acesso em 27 ago. 2019.
- 67 INTERVOZES. **Contribuições para uma regulação democrática das grandes plataformas que garanta a liberdade de expressão na internet.**, 2019. p. 4. Disponível em: <<https://bit.ly/2kFRYHp>>. Acesso em: 13 set. 2019.
- 68 YOUTUBE. **Policies and Safety**. Disponível em <<https://bit.ly/2kOdmUv>>. Acesso em 17 set. 2019.
- 69 HENRY, Daniel. **Media and the Law**. Disponível em <<https://bit.ly/2IN8lMe>>. Acesso em 13 set. 2019
- 70 SHIEBER, Jonathan. **Australia passes law to hold social media companies responsible for "abhorrent violent material"**. Disponível em <<https://tcn.ch/2uQS22e>>. Acesso em 13 set. 2019.
- 71 KURBALIJA, Jovan. **Uma introdução à governança da internet**. São Paulo:

Comitê Gestor da Internet no Brasil, 2016. P. 51. Disponível em <<https://bit.ly/31WYVgf>>. Acesso em 30 set. 2019.

72 ATKIN, David J.; JEFFRES, Leo W.; NEUENDORF, Kimberly A. **Understanding Internet adoption as telecommunications behavior**. Journal of Broadcasting & Electronic Media, v. 42, n. 4, p. 475-490, 1998.

73 INTERVOZES. **Contribuições para uma regulação democrática das grandes plataformas que garanta a liberdade de expressão na internet**: Uma perspectiva latino-americana para alcançar processos de moderação de conteúdo compatíveis com os padrões internacionais de direitos humanos. Disponível em: <<https://bit.ly/2kfRYHp>>. Acesso em: 22 out. 2019.

74 HARRIS, Brent. **Establishing Structure and Governance for an Independent Oversight Board**. Disponível em <<https://bit.ly/2mlgY0H>>. Acesso em 22 out. 2019.

75 BRASIL. **Leinº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, Disponível em: <<https://bit.ly/1kxaoKm>>. Acesso em: 22 set. 2019.

## 2. PROBLEMÁTICAS



## 2. PROBLEMÁTICAS

### 2.1. Apropriação de tecnologias

Segundo Cristina Kiomi Mori<sup>76</sup>, o conceito de Inclusão digital pode ser compreendido a partir de três aspectos: i) acesso - que se relaciona a questões de infraestrutura; ii) alfabetização digital - desenvolvimento de habilidades que permitam o uso pleno das tecnologias da informação e comunicação (TICs); e iii) apropriação de tecnologias. A apropriação das TICs é o fim último da inclusão digital para essa terceira abordagem e acontece quando os indivíduos têm acesso e domínio, compreendem o significado das dimensões técnicas e deixam de consumir passivamente para atuarem como cocriadores, explorando as ferramentas e atribuindo a elas novas funcionalidades.

### 2.2. Assédio on-line

Pode ser entendido como um aborrecimento, insulto, ameaça ou qualquer comportamento ofensivo endereçado de forma repetida ou não a outro indivíduo por meio das plataformas digitais.

Ao escrever sobre as especificidades do assédio por meio de plataformas online, Peter<sup>77</sup> ressalta o fato de que muitas vezes a internet favorece o anonimato. O autor destaca que no exercício da **moderação do**



**conteúdo** veiculada na rede, os operadores de plataforma desempenham importante posição de encorajar ou de desencorajar certas práticas na rede por meio da vedação de comportamentos nas políticas e padrões de suas interfaces. Um outro ponto sensível dessa discussão é que compreender e delimitar os limites entre liberdade de expressão e assédio nem sempre é uma tarefa simples. Problemas como cyberbullying, discurso de ódio, assédio moral e sexual são recorrentemente relatados, como é possível verificar a partir de canais de denúncia como o da Safernet Brasil<sup>78</sup>.

Em um estudo sobre as características que tornam o assédio mais problemático e agressivo aos jovens, Kimberly J. Mitchell entre outros autores<sup>79</sup> demonstram que fatores como o envolvimento de múltiplos atores, bem como o acúmulo de recursos agravantes (se as pessoas envolvidas têm contato offline, se há repetição, se envolve relações de poder e hierarquia etc.) potencializam o poder destrutivo da atividade.

O relatório de uma pesquisa sobre assédio online realizada nos Estados Unidos em 2017 demonstrou<sup>80</sup> que a maior parte dos assédios se constroem sobre características físicas ou pessoais, como aparência física, posicionamento político, gênero e raça.

Compreender os fatores que configuram essa prática é importante para educadores, pais e demais pessoas dedicadas à prevenção do assédio online, com a atenção às pessoas afetadas.

### 2.3. Ciberbullying

É uma das formas mais recorrentes de assédio online entre crianças e adolescentes. A prática do bullying já encontrava rastro nos ambientes escolares, entretanto, com a proliferação do uso da internet, que se tornou espaço de interações positivas e negativas - assim como no “mundo offline” - o ciberbullying se revelou um novo problema. Segundo os autores Espelage e Swearer<sup>81</sup>, há número considerável de definições sobre o que se entende por bullying. Um ponto comum entre a maior parte das discussões é que se trata de uma forma de agressão. E, comumente são encontradas definições que o caracterizam como uma ação negativa e repetida de um ou mais estudantes contra uma outra parte em situação de maior vulnerabilidade. Recorrentemente, os casos são caracterizados por agressões verbais, humilhação, exposição, violência emocional, exclusão e isolamento, entre outras.

O compartilhamento de conteúdo que causa humilhação, ofensa, ameaça, é previsto como crime na Lei nº 13185/2015<sup>82</sup> e deve ser denunciado.

Segundo os estudos de Dadvar<sup>83</sup>, o bullying online pode ser mais danoso e causar problemas mais duradouros do que o offline, uma vez que o conteúdo lançado na rede se prolifera de forma acelerada, aumentando seu alcance e envolvendo maior exposição, além de que o conteúdo escrito pode ficar registrado por muito tempo e a ofensa pode ser lida várias vezes pela vítima.

## 2.4. Desinformação

Desinformação, ou desordem informacional é o problema causado pela má compreensão ou absorção de uma informação, seja por disseminação de informação distorcida, tendenciosa, sem rastro na realidade, por falhas comunicativas na emissão e interpretação de uma mensagem. Nos últimos anos, o tema ganhou destaque e se tornou um problema generalizado. Em um relatório de 2013<sup>84</sup>, o Fórum Econômico Mundial apontou a desinformação como um dos grandes desafios da sociedade contemporânea. No texto, a questão é comparada a um incêndio, que pode causar muita destruição no mundo físico até que seja apagado. A desinformação traz consequências políticas, econômicas, sociais e materiais diretas e pode colocar a integridade de pessoas em risco.

Em 2019, a Organização das Nações Unidas para a Educação, a Ciência e Cultura (UNESCO), publicou um manual para Educação e treinamento em Jornalismo: “Jornalismo, fake news e desinformação”. Nele, a instituição organizou em sete tópicos diferentes fontes de desordem informacional.<sup>85</sup>

1. Sátira ou paródia: feito sem intenção de enganar, mas que pode causar confusão.
2. Conteúdo enganoso: usa-se da imagens, citações ou estatísticas de

forma seletiva.

3. Conteúdo impostor: propaga-se uma informação em nome de outra fonte, forjando a assinatura.
4. Conteúdo fabricado: informação completamente inventada com intenção de enganar.
5. Conexão falsa: Imagens ou legendas não correspondem ao conteúdo.
6. Contexto falso: conteúdo verdadeiro, porém deslocado de seu contexto de origem. Por exemplo, quando se utiliza uma foto de um determinado país para ilustrar um texto que fala sobre outro.
7. Conteúdo manipulado: fatos e imagens verdadeiras são modificadas com intenção de enganar.

A abundância informacional transformou a maneira como nos comunicamos, interagimos e nos informamos. Um estudo de 2015<sup>86</sup> sobre como usuários interagem com notícias no Facebook provenientes de canais científicos ou alternativos demonstrou que a tendência de que os indivíduos se cerquem de pessoas ideologicamente próximas e a propensão da rede em formar grandes bolhas de interesse, o que chamamos de polarização, favorecem que indivíduos acreditem mais facilmente nas informações que circulam nessa rede.

De acordo com estudo conduzido por Lewis, o algoritmo utilizado pelo Youtube pode ter influenciado enfaticamente a proliferação de desinformação e teorias conspiratórias. A ferramenta de sugestão de próximos vídeos utilizada pelo site se baseia no interesse do espectador a fim de mantê-lo entretido por mais tempo na plataforma.<sup>87</sup> O algoritmo tende a recomendar vídeos que reforçam o ponto de vista que está sendo visualizado e cria uma bolha de filtro, favorecendo a polarização e o fortalecimento de conteúdos que promovem a desinformação. Um estudo realizado por **Meira** e outros autores auditou algoritmos de recomendação de próximos vídeos com objetivo de avaliar tendências à radicalização, fez uma auditoria do algoritmo de recomendação de próximos vídeos do Youtube para avaliar se havia uma tendência à radicalização. Os resultados encontrados demonstram que há uma tendência à radicalização dos usuários na plataforma, na medida em que há uma migração significativa para o consumo de conteúdos mais radicais polarizados à extrema direita, no entanto, por não considerarem o fator personalização e não terem acesso ao funcionamento do sistema nos períodos anteriores, o grupo de pesquisadores acusa não ser possível determinar a extensão do papel do algoritmo de recomendação nesse movimento de polarização. Os pesquisadores argumentam, ainda, que isso pode ser impulsionado pela recusa dos meios de comunicação tradicional e grande mídia e pelo aumento do fluxo de conteúdo no feed das redes sociais.<sup>88</sup>

## 2.5. Discurso de ódio

Discurso de ódio diz respeito a manifestações que podem gerar danos morais e emocionais. Segundo Winfred Brugger, são palavras que tendem a insultar a violência, assédio e hostilidade contra determinados grupos ou a uma pessoa. É uma forma de violência baseada em critérios discriminatórios como raça, gênero, religião, orientação sexual, entre outros<sup>89</sup>.

O discurso de ódio busca não apenas insultar, mas também incitar novas violações contra direitos fundamentais e a dignidade de indivíduos ou da coletividade. Ainda que possa ser direcionado a uma única pessoa, o discurso odioso, ao discriminar características específicas, causa danos a todos os demais indivíduos que compartilham da mesmas características<sup>90</sup>.

Ainda que discursos odiosos possam ser realizados em diferentes meios de comunicação, a internet proporciona um potencial significativamente maior não somente de visibilidade, mas também de interação entre os discursos. Assim, o discurso de ódio encontra na rede mundial de computadores um ambiente conveniente à incitação de mais pessoas a corroborar práticas de discriminação, como por meio de caixas de comentários e compartilhamentos de postagens.

Apesar de a liberdade de expressão ser considerada um direito fundamental previsto na Constituição Federal e no Marco Civil da

Internet (Lei 12.956/2014), seu exercício não deve ferir outros direitos. Assim como outros direitos que devem ser sopesados, a liberdade de expressão não é absoluta e deve preservar os direitos à personalidade - honra, privacidade, intimidade e imagem de alguém - ou a dignidade da pessoa humana.

## 2.6. Exclusão digital

Conceito em oposição à inclusão digital. Exclusão digital se relaciona à condição dos sujeitos que não tiveram oportunidade de acesso a inclusão digital. Em consonância com outros conceitos apresentados neste glossário (e também em seu primeiro Volume<sup>91</sup>), entende-se como inclusão digital não somente a possibilidade do acesso às ferramentas e infraestrutura, mas também a aquisição de competências de letramento digital que permitam uma usabilidade plena e consciente das ferramentas digitais<sup>92</sup>. Na literatura sobre o tema, também é encontrado o termo sinônimo “infoexclusão”.

Autores têm apontado para a correlação entre exclusão social e exclusão digital<sup>93</sup>, demonstrando que a oportunidade e o acesso às tecnologias digitais variam de acordo com condições socioeconômicas dos indivíduos, sobretudo em países que apresentam marcas de desigualdade profundas, como é o caso brasileiro. A pesquisa sobre o acesso à internet a partir dos domicílios brasileiros em 2017<sup>94</sup> do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br) - órgão brasileiro responsável por monitorar a incorporação

\* O Cetic usou o Critério de Classificação Econômica Brasil 2015, disponível online, que apresenta um modelo estatístico de classificação socioeconômica dos cidadãos com base na posse de bens materiais e nível de instrução do (da) chefe da família.

de tecnologias da informação em diversos setores da sociedade - demonstrou a discrepância entre o acesso à internet entre as diferentes classes regiões brasileiras. A partir dos dados coletados, observa-se que metade dos domicílios localizados em área urbana dispunham de um computador, ao passo que, na zona rural, essa margem alcançou somente os 24%. E, ainda, que 98% dos indivíduos classe A\* possuíam computador com acesso à internet em casa, enquanto que, entre os cidadãos de classe DE, 7% dos domicílios tinham computador conectado à rede<sup>95</sup>.

## 2.7. Fake news (“notícias falsas”)

As fake news são um dos tipos de desinformação, pois, enquanto uma notícia verdadeira que é divulgada fora do contexto pode gerar um entendimento diferente do verdadeiro, ou seja, gerar desinformação, as fake news, por sua vez, mobilizam e propagam narrativas inverídicas. O compartilhamento de fake news é um problema para toda a comunidade digital, uma vez que gera mal entendidos, transtornos, danos políticos, sociais e econômicos. O termo, no entanto, é considerado paradoxal e tem sido evitado, uma vez que pelo termo “notícia”, entende-se uma informação verificável e de interesse público. Assim, se um fato mentiroso é disseminado como verdade, não se trata de uma notícia propriamente dita.<sup>96</sup>



## 2.8. Processo de inclusão excludente

Diversos programas governamentais, da sociedade civil e do setor empresarial têm como objetivo ampliar a inclusão digital. Entretanto, certas iniciativas oferecem apenas algumas das ferramentas que são necessárias para efetiva inclusão digital. Quando os recursos disponibilizados para o cidadão não são acompanhados pelo aparato necessário para o uso consciente, responsável e crítico da tecnologia, é possível que a pretensão de inclusão digital reforce condições de marginalização. Assim, o indivíduo é incluído em um ambiente de condições precárias<sup>97</sup>.

O Programa um computador por aluno (PROUCA)<sup>98</sup> é considerado por parte da literatura como um exemplo de processo de inclusão digital excludente. Instituído em 2010, o PROUCA pretendia aumentar a qualidade da educação por meio da inclusão digital. Entretanto, o programa apenas considerou um dos aspectos que permeiam o processo de inclusão digital: a aquisição de um computador.

Entre as críticas tecidas ao programa, destaca-se a desigualdade de participação escolar entre os alunos que possuíam computadores e internet de qualidade em suas casas, ou seja, detinham domínio da tecnologia, e alunos que tinham acesso à máquina apenas durante o período escolar<sup>99</sup>. Além disso, assim como apontado por Echalar e Peixoto, não houve adequada

formação dos professores para o uso pedagógico dos computadores em sala de aula. Portanto, os autores consideram que o PROUCA aproximou-se das ações que constroem demanda do indivíduo por determinados bens e serviços<sup>100</sup>, no caso bens digitais e tecnológicos, não sendo efetivo ao favorecimento da melhoria da renda e o acesso à educação.

## 2.9. Aliciamento on-line

\* O código penal brasileiro emprega a palavra aliciamento em dois artigos para proibir que trabalhadores sejam recrutados para trabalhar no exterior em condições diferentes das apresentadas inicialmente pelo recrutador. Além disso, no art. 218, 227, 228 o Código Penal também se refere ao aliciamento, para proibir a indução de menores a satisfazer a libido de outrem ou à prostituição. Os artigos recém mencionados compõem o rol de crimes relacionados ao abuso sexual.

A palavra aliciamento significa atração de indivíduos ou grupos para prática de determinada atividade. Ainda que o significado originário<sup>101</sup> da palavra não esteja necessariamente relacionado a condutas criminosas, a expressão “aliciamento” é, de modo majoritário, utilizada para se referir a indução à práticas proibidas\*.

O advento da internet proporcionou e proporciona que o conhecimento seja disseminado para mais pessoas e de forma mais rápida. Assim, a disponibilização de informações sobre os aspectos e como denunciar formas de aliciamento relacionadas à exploração de trabalho e abusos sexuais é útil para o combate a esses crimes. Destaca-se a campanha #PODESERABUSO<sup>102</sup>, que por meio de vídeos e postagens nas redes sociais busca orientar crianças e pais sobre o assunto.

A comercialização da internet também possibilitou que condutas nocivas atinjam mais vítimas. O aliciamento, especialmente o aliciamento de crianças e adolescentes

para satisfação de prazeres sexuais de um adulto, também ganhou novas conotações e se desenvolve de maneiras diferentes quando a comunicação entre aliciador e vítima inicia-se pela internet. Maria Emília Brentam utiliza o termo violência sexual mediada por TIC para se referir ao “aliciamento para fins de abuso, exploração sexual e tráfico internacional de seres humanos e o abuso sexual on-line”<sup>103</sup>.

A infância abrange as primeiras fases do desenvolvimento cognitivo e sensorial do indivíduo. Portanto, por não terem plena capacidade para avaliar riscos e consequências de comportamentos controversos, as crianças e adolescentes são considerados grupos que demandam especial atenção e proteção pela sociedade. Além disso, em geral, pessoas com menor poder aquisitivo fazem uso da internet com pouca informação a respeito dos riscos e formas de proteção on-line. Portanto, para Brentam, entre os grupos que estão mais expostos ao risco do aliciamento sexual on-line, destaca-se como grupo mais vulnerável as crianças de classes sociais mais baixas<sup>104</sup>.

O aliciamento de crianças na internet para fins sexuais é um crime com certo padrão consistente e que exige sutileza e aproximação progressiva por parte do aliciador. Para O’Connell<sup>105</sup>, a maneira como os agressores abordam crianças em redes sociais ou sala de bate-papos perpassa os seguintes estágios: 1. Formação da amizade; 2. Formação do relacionamento; 3. Avaliação de risco; 4. Estágio de exclusividade – amor e confiança mútuo; 5. Estágio sexual.

A organização Safernet<sup>106</sup> atua diretamente com o enfrentamento do aliciamento on-line de crianças, por meio da produção de cartilhas e atividades educacionais, bem como recebendo denúncias de atividades ilícitas desse tipo e encaminhado ao Ministério Público. Para o combate ao crime de aliciamento, especialmente o sexual envolvendo crianças e adolescentes, algumas ferramentas tecnológicas podem ser úteis, como o **controle de acesso parental**. Entretanto, é essencial que os usuários da internet conheçam as boas práticas para a utilização da internet de forma consciente e responsável, além do efetivo acompanhamento dos pais ou tutores das crianças sobre as atividades realizadas no ambiente virtual.<sup>107</sup>

## 2.10. Phishing e golpes

Usuários mal intencionados da internet por vezes exploram fragilidades de outros usuários com a intenção de obter vantagem econômica. Para tanto, os agentes utilizam técnicas de engenharia social. A combinação da teoria de Mitnick, Simon<sup>108</sup> e Mann<sup>109</sup>, conforme analisada por Geraldo e Takeda, define “engenharia social como métodos de influenciar ou persuadir pessoas com o intuito de convencê-las a fornecer informações sigilosas de uma organização ou pessoal”<sup>110</sup>. Por incidirem no âmbito econômico do cidadão, muitos golpes realizados na internet são crimes contra o patrimônio e classificados como estelionato\*.

\* Estelionato

Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:

Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.

Entre as atividades maliciosas destacam-se o envio de mensagens eletrônicas falsas,

criação de empresas fantasmas e de contas bancárias ilegítimas. Quanto aos golpes mais praticados, constam: i) furto de identidade, ii) golpes de comércio eletrônico - que inclui desde a hospedagem de um site fraudulento de compra e venda de mercadoria pela internet até participantes de leilão que utilizam os dados financeiros do vendedor para outros fins, e iii) boatos (hoax)<sup>111</sup>. O phishing também consta na lista de golpes e é utilizado em 90% dos roubos de informações pessoais pela internet<sup>112</sup>.

Phishing é uma forma de ataque semântico, ou seja, por meio de mensagens enganosas direcionadas ao usuário o agente do ataque tem acesso a informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias. Como exemplos de situações envolvendo phishing, destacam-se o envio de mensagens falsas em nome de instituições bancárias reais solicitando informações financeiras e a disponibilização de um link sobre compra de passagens aéreas de companhias reais que direcionam ao preenchimento de formulários, que encaminham os dados informados para os golpistas<sup>113</sup>.

O Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT), mantido pelo NIC.br, disponibiliza uma cartilha on-line<sup>114</sup> com diversas estratégias para os usuários da internet se prevenirem dos golpes mencionados anteriormente. A criação de senhas fortes, utilização de sites que implementaram o protocolo https e utilização

de mecanismos de segurança, como programas antimalware e firewall pessoal são algumas das ferramentas para proteção dos usuários na rede.

## 2.11. Sexting

Troca de conteúdos de cunho sexual por meio de **plataformas online**, como a troca de mensagens, fotos ou vídeos. A prática oferece riscos pois, uma vez que o conteúdo é lançado na internet, poderá ser compartilhado e replicado, gerando transtorno para a pessoa que teve a sua privacidade violada e causar traumas. Uma vez postado na internet, o conteúdo pode não ser removido tão facilmente. A prática também se relaciona com atividades criminosas como o **aliciamento** ou a **pornografia de revanche**.

Em 2015, a ONG Coding Rights lançou um zine chamado “Safer Nudes – Guia Sensual de Segurança Digital”, apresentando ferramentas de criptografia e segurança da informação como boas práticas e cuidados no compartilhamento de fotos íntimas. O material está disponível online no site da instituição.<sup>115</sup>

## 2.12. Cyberstalking

Originado do termo stalking, que do inglês significa “perseguir”, o cyberstalking se refere a uma forma de assédio online na qual a prática da perseguição é realizada a partir da internet. Em termos gerais, essa forma de assédio é entendida como um padrão de comportamentos de alguém

que insistentemente causa medo em sua vítima, a fim de exercer controle sobre ela - procedimentos possíveis de serem realizados tanto no “mundo offline” quanto na internet<sup>116</sup>. De acordo com Paul Bocij e Leroy McFarlane, o cyberstalking pode englobar comportamentos como ameaças, falsas acusações, roubo de identidade e/ou dados, danos a equipamentos, monitoramento de computadores e apelos sexuais a menores de idade<sup>117</sup>. É importante salientar que o cyberstalking é capaz de trazer sérios danos, não apenas psicológicos, mas também físicos às vítimas.

Na Lei Brasileira, a perseguição consta até então como contravenção penal<sup>118</sup>, e não crime. De acordo com o artigo 65 da Lei de Contravenções Penais, a perseguição é definida como “molestar alguém ou perturbar-lhe a tranquilidade, por acinte ou por motivo reprovável”, com pena prevista de prisão simples, de quinze dias a dois meses, ou multa. Apesar disso, é importante ressaltar que o Artigo 147 do Código Penal brasileiro considera a ameaça - seja por palavras, escritos, gestos ou outro meio simbólico - como crime contra a liberdade pessoal<sup>119</sup>, com pena prevista de detenção de um a seis meses ou multa.

Atualmente, o Projeto de Lei n. 3.484, de 2019, busca criar o crime de “Perseguição Insidiosa ou Obsessiva”, definido como o ato de “perseguir, importunar ou perturbar a tranquilidade de alguém, reiteradamente, ainda que por meio da internet, de modo a causar-lhe danos de ordem psicológica,

moral ou social, violando seus direitos de liberdade, privacidade ou segurança”<sup>120</sup>.

### 2.13. Uso excessivo da internet

Problema encontrado quando as demais atividades e/ou saúde de um usuário passam a ficar comprometidas pelo uso excessivo da internet, podendo causar dependência. O tempo exagerado dispensado nas redes pode prejudicar o desempenho do indivíduo no trabalho ou nos estudos, levar a dificuldade de concentração, interação social, alimentação, sono, entre outras tarefas comuns a todas as pessoas. Em um artigo de revisão bibliográfica sobre o tema, Abreu e outros autores discorrem sobre como o problema tem sido tratado pela psiquiatria desde 1995, com um crescente número de casos e demanda por tratamento<sup>121</sup>. Os autores apresentam outros termos que têm sido utilizados para falar do mesmo problema, como: vício em internet, uso patológico da internet, transtorno de vício em internet, uso compulsivo da internet, viciados em comunicações mediadas por computador, viciados em computador e dependência de internet (tradução nossa)<sup>122</sup>. Entretanto, o estudo também aponta que se trata de uma diversidade de abordagem por diferentes profissionais interessados nesta questão, o que justifica enfoques distintos e, conseqüentemente, termos diferentes.

O Hospital das Clínicas de São Paulo oferece, desde 2006, o serviço de atendimento



e tratamento às pessoas que estejam passando por dificuldades na administração do tempo que despendem em plataformas online, além de desenvolverem pesquisa na área. Entre as informações encontradas no site do ambulatório integrado de controle dos impulsos, há a indicação dos sintomas que devem alertar para uma situação de dependência da internet, caso se observe mais do que cinco deles:

1. Preocupação excessiva com a internet;
2. Necessidade de aumentar o tempo conectado (on-line) para ter a mesma satisfação;
3. Exibir esforços repetidos para diminuir o tempo de uso da internet;
4. Apresentar irritabilidade e/ou depressão;
5. Quando o uso da internet é restringido, apresenta labilidade emocional (internet como forma de regulação emocional);
6. Permanecer mais conectado (on-line) do que o programado;
7. Ter o trabalho e as relações familiares e sociais em risco pelo uso excessivo;
8. Mentir aos outros a respeito da quantidade de horas conectadas.<sup>123</sup>

\* Art. 29. O usuário terá a opção de livre escolha na utilização de programa de computador em seu terminal para exercício do controle parental de conteúdo entendido por ele como impróprio a seus filhos menores, desde que respeitados os princípios desta Lei e da Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, de conteúdos de réis.

## 2.14. Controle parental

É uma das estratégias para garantir a segurança on-line da criança e do adolescente por meio da contenção ou administração, por parte dos pais, de sites, sistemas operacionais e dispositivos utilizados por crianças<sup>124</sup>. Além disso, o Marco Civil da Internet\*, lei que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil<sup>125</sup>, estimula que sejam utilizadas ferramentas de controle parental para assegurar o uso seguro da internet por parte de crianças e adolescentes.

Destaca-se a importância das ferramentas de controle parental serem utilizadas de modo condizente com as liberdades e direitos das crianças e adolescentes, e sua proteção integral, de modo a propiciar que o uso da internet seja ponte para o desenvolvimento e expressão criativa, intelectual e social.

Segundo a Researchandmarkets<sup>126</sup>, o mercado global de controle parental será avaliado em USD 3.3 milhões em 2025. As principais ferramentas de controle parental são:

1. Seleção de faixas etárias permitidas às crianças;
2. Controle e monitoramento das compras digitais efetuadas;
3. Limitação ao acesso à internet por

meio da aplicação de filtros;

4. Controle da quantidade de tempo gasto pelas crianças jogando;
5. Controle dos níveis de interação (chat) e trocas de dados (mensagens de texto).<sup>127</sup>

Estudos empíricos apontaram que o uso e relação das crianças com a internet é diretamente associada aos estilos sociais e de uso que os pais ou responsáveis fazem da internet<sup>128</sup>. Portanto, para além do uso de ferramentas e de softwares de controle parental, pais e tutores devem atuar na educação dos menores para uso consciente e responsável das tecnologia da informação e comunicação (TIC), além de conhecerem o funcionamento das tecnologias, tanto de um computador quanto de um smartphone<sup>129</sup>.

## 2.15. Pornografia de revanche

Conduta criminosa relacionada à divulgação de conteúdo íntimo (fotos, conversas, vídeos) na rede sem o conhecimento nem o consentimento da pessoa envolvida. Recorrentemente, a prática acontece após uma situação de término de relacionamento e, por isso se associa a um tipo de revanchismo. Entretanto, como apresentado por Neris, Ruiz e Valente<sup>130</sup>, em muitos outros casos não há envolvimento da figura de um ex-parceiro, e não precisa que o seja para configurar um ato criminoso. Por isso, segundo as autoras, o termo

mais adequado seria “disseminação não consentida de imagens íntimas”.

Os enormes danos causados por tal prática levaram à mobilização da legislação de diversos países para punição a conduta. No artigo “Análise comparada de estratégias de enfrentamento a ‘revenge porn’ pelo mundo”, as autoras Neris, Ruiz e Valente fazem um levantamento das sanções adotadas em 27 países, inclusive no Brasil, onde a conduta foi definida como crime contra a honra, crime contra a liberdade pessoal, crime contra a liberdade sexual e, também há casos que se aplica a Lei Maria da Penha, quando o há vínculo afetivo.<sup>131</sup>

## 2.16. Anonimato

De acordo com Capanema, “O anonimato é a manifestação de vontade sem a indicação ou referência do seu autor, sem que se possa individualizá-lo ou determiná-lo”<sup>132</sup>. Em 1993, o cartunista Peter Steiner cunhou a célebre frase “Na internet, ninguém sabe que você é um cachorro” fazendo referência à pouca informação que se tinha sobre o usuário da internet na época, o que aproximava os usuários de um sujeito anônimo. Entretanto, como Machado afirma, as mudanças ocorridas nas redes digitais após 1990 findaram com o estabelecimento do usuário-anônimo como regra<sup>133</sup>. Principalmente com a eclosão das redes sociais, as plataformas digitais passaram a priorizar a participação do usuário por meio do uso de seu nome identificado em sua vida cotidiana.

\* Entre os instrumentos disponíveis para garantia o anonimato do usuário da rede, destaca-se o uso de rede virtual privada (VPN) ou programas como TOR – The Onion Network, que servem para ocultar a identificação do computador, além do uso de criptografia nos dispositivos computacionais.

A utilização de dados identificáveis, tais como o endereço IP, metadados, informações de registro (log), nomes verdadeiros na navegação favorece “a precisa identificação do usuário da internet com vistas ao controle e repressão de comportamentos ilícitos e ofensivos”<sup>134</sup>. Entretanto, existe uma corrente que aponta situações em que o anonimato deve ser preservado para garantia da liberdade de expressão\*. A título de exemplo, Capanema menciona diversas denúncias de abusos cometidos pelo Estado, as quais foram publicadas por usuários da rede utilizando seus nomes verdadeiros e, após as denúncias on-line, foram perseguidos<sup>135</sup>.

CAPANEMA, Walter Aranha. O direito ao anonimato: uma nova interpretação do art. 5º, IV, CF. A voz do cidadão, 2017. Disponível em <<https://bit.ly/2kFKFZY>>. Acesso em 23 set. 2019.

## 2.17. Superexposição

Apostagem de conteúdos que apresentem informações ou posicionamentos pessoais em plataformas da internet como sites, blogs e redes sociais, é considerada exposição dos usuários. Dessa forma, a superexposição é caracterizada como o excesso dessa prática.

Além de **plataformas digitais**, as redes sociais também são ambientes de socialização mediados pela internet<sup>136</sup>, em que usuários constroem suas identidades e expressam suas personalidades por meio da interação social online<sup>137</sup>. Nesse processo, a prática de postar aparece como uma forma de conexão entre atores sociais e o estreitamento de seus laços sociais<sup>138</sup>. Pesquisadores da universidade de Monash, na Austrália, apontam que existem três principais razões que perpetuam o comportamento de exposição na internet:

autoexpressão, necessidade de atenção e busca por popularidade.<sup>139</sup>

## 2.18. Vigilantismo

Os “vigilantes”, ou “justiceiros”, são pessoas organizadas na rede para reagirem a comportamentos que julgam recrimináveis. Geralmente, as ações são direcionadas a grupos criminosos, corruptos, redes de exploração infantil, entre outras. Ao encontrarem um conteúdo ofensivo aos seus princípios na rede, essas pessoas tentam identificar os responsáveis e encaminhar para autoridades investigativas e do Poder Judiciário, além de denunciar o conteúdo para que seja retirado do ar. Os grupos articulados para esse fim entendem que é preciso fazer frente à ineficiência do Estado em assegurar o funcionamento ordenado da justiça e a reagir em situações de desordem. Por isso, muitas vezes, esses atores têm a capacidade de mobilização maior e mais rápida do que as vias burocráticas institucionais. Tal prática, no entanto, se apresenta como uma problemática quando exprime intenções de revanche, com linchamentos virtuais e assédio. Assim, os justiceiros passam a cometer crimes para combater o crime. O termo também é encontrado como cibervigilantismo, digilantismo ou vigilantismo digital.<sup>140</sup>

Em um artigo sobre a prática do vigilantismo no meio digital, ressaltando as questões de vigilância e exposição envolvidas, o autor Daniel Trottier aponta, entre outras coisas, que a prática do vigilantismo tenciona

uma visibilidade com três características. Ela é indesejada pelo o alvo; é intensa, com produção e disseminação de conteúdo de forma exaustiva; e, finalmente, duradoura, podendo deixar associada por um bom tempo a figura alvo ao seu ato recriminado<sup>141</sup>.

## NOTAS

76 MORI, Cristina K. **Políticas públicas para inclusão digital no Brasil**: aspectos institucionais e efetividade em iniciativas federais de disseminação de telecentros no período 2000-2010, (2011). Disponível em <<https://bit.ly/2maPE97>>. Acesso em 10 set. 2019.

77 PATER, Jessica et al. **Characterizations of Online Harassment**: Comparing Policies Across Social Media Platforms. Disponível em <<https://bit.ly/2klrwwg>>. Acesso em 02 de ago. 2019.

78 SAFERNET. **Hotline**. Disponível em <<https://bit.ly/2zYwmo5>>. Acesso em 22 out. 2019

79 MITCHELL, Kimberly J. et al. **What features make online harassment incidents upsetting to youth?**. Journal of school violence, v. 15, n. 3, p. 279-301, 2016. Disponível em <<https://bit.ly/2lSHKNS>>. Acesso em 02 ago. 2019.

80 DUGGAN, Maeve. **Online harassment**. Pew Research Center, 2014. Disponível em <<https://pewrsr.ch/2kzia02>>. Acesso em 02 ago. 2019

81 ESPELAGE, Dorothy L.; SWEARER NAPOLITANO, Susan M. **Research on school bullying and victimization**: What have we learned and where do we go from here?[Mini-series]. 2003 Disponível em <<https://bit.ly/2lTmzlg>>. 02 ago. 2019.

82 BRASIL. **LEI Nº 13.185, de 6 de novembro de 2015, Institui o Programa de Combate à Intimidação Sistemática (Bullying)**. Disponível em: <<https://bit.ly/2PX1P0J>>. Acesso em: 13 nov. 2019.

83 DADVAR, Maral; DE JONG, Franciska. **Cyberbullying detection**: a step toward a safer internet yard. In: Proceedings of the 21st International Conference on World Wide Web. ACM, 2012. p. 121-126. Disponível em <<https://bit.ly/2kgm25L>>. Acesso em 02 ago. 2019.

84 HOWELL, Lee et al. **Digital wildfires in a hyperconnected world**. WEF report, v. 3, p. 15-94, 2013.

85 IRETON, Cherilyn; POSETTI, Julie (Org.). **Jornalismo, Fake News & Desinformação**: Manual para Educação e Treinamento em Jornalismo. Paris: Organização das Nações Unidas Para A Educação, A Ciência e A Cultura (unesco), 2019. 129 p. Tradução de Sarah Rebouças Reedman. Disponível em: <<https://bit.ly/2MWUON0>>. Acesso em: 03 set. 2019.

86 BESSI, Alessandro et al. **Science vs conspiracy**: Collective narratives in the age of misinformation. PloS one, v. 10, n. 2, p. e0118093, 2015. Disponível em <<https://bit.ly/2lMZZvM>>. Acesso em 04 set. 2019.

87 LEWIS, Paul. 2018. **'Fiction is outperforming reality'**: how YouTube's algorithm distorts truth. The Guardian, Fevereiro, 2018. Disponível em <<http://bit.ly/2EqBq8p>> acesso em 12 set. 2019.



- 88 RIBEIRO, Manoel Horta et al. **Auditing Radicalization Pathways on YouTube**. 2019. Disponível em: <<https://arxiv.org/abs/1908.08313>>. Acesso em: 28 nov. 2019.
- 89 BRUGGER, Winfried. **Proibição ou proteção do discurso do ódio?** Algumas observações sobre o direito alemão e o americano. Trad. Maria Angela Jardim de Santa Cruz Oliveira. Revista de Direito Público, v. 15 n. 117, jan./mar. 2007, p. 118. Disponível em: <<https://bit.ly/2m9mZnQ>>. Acesso em: 10 set 2019.
- 90 SILVA, Rosane L; NICHEL, Andressa; MARTINS, Anna C. L; BORCHARDT, Carlise K. **Discursos de ódio em redes sociais:** jurisprudência brasileira. Rev. direito GV [online]. 2011, vol.7, n.2, p. 445-468. Disponível em: <<https://bit.ly/2m8A7CQ>>. Acesso em: 10 set. 2019.
- 91 CARMO, Paloma; DUARTE, Felipe; GOMES, Ana Bárbara. **Glossário da Inclusão Digital - Volume I**. Instituto de Referência em Internet e Sociedade: Belo Horizonte, 2019. Disponível em: <<https://bit.ly/2Ev9zBJ>>. Acesso em: 10 out. 2019.
- 92 SILVA, Bento Duarte da; PEREIRA, Maria da Graça Caridade Barbosa. **O papel da escola no combate à divisão digital**. In: XI Congresso Luso Afro Brasileiro de Ciências Sociais: diversidades e (des) igualdades. Universidade Federal da Bahia (UFBA), 2011. Disponível em <<https://bit.ly/2kK9DY6>>. Acesso em 06 set. 2019.
- 93 DA SILVA, Ângela Carrancho. **Educação e tecnologia:** entre o discurso e a prática. Ensaio: avaliação e políticas públicas em educação, v. 19, n. 72, p. 527-554, 2011. Disponível em <<https://bit.ly/2mc1zj6>>. Acesso em 09 set. 2019
- 94 NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), **Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nos domicílios brasileiros** - TIC Domicílios 2018. Disponível em <<https://bit.ly/330YvHe>>, acesso em 09 set. 2019.
- 95 NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), **Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nos domicílios brasileiros** - TIC Domicílios 2018. A4B - DOMICÍLIOS, POR PRESENÇA DE COMPUTADOR E INTERNET. Disponível em <<https://bit.ly/2M8n26N>>, acesso em 09 set 2019.
- 96 IRETON, Cherilyn; POSETTI, Julie (Org.). **Jornalismo, Fake News & Desinformação:** Manual para Educação e Treinamento em Jornalismo. Paris: Organização das Nações Unidas Para A Educação, A Ciência e A Cultura (unesco)., 2019. 129 p. Tradução de Sarah Rebouças Reedman. Disponível em: <<https://bit.ly/2rYoQlw>>. Acesso em: 03 set. 2019.
- 97 KUENZER, Acácia Zeneida. **Da dualidade assumida à dualidade negada:** o discurso da flexibilização justifica a inclusão excludente. Educação & Sociedade, v. 28, n. 100, p. 1153-1178, 2007. Disponível em <<https://bit.ly/2kKaFDs>>. Acesso em 13 set. 2019.
- 98 MINISTÉRIO DA EDUCAÇÃO. **Programa um computador por aluno (PROUCA)**. Disponível em <<https://bit.ly/2Lrxo0z>>. Acesso em 13 set. 2019

- 99 ECHALAR, Adda Daniela Lima Figueiredo; PEIXOTO, Joana. **Programa Um Computador por Aluno**: o acesso às tecnologias digitais como estratégia para a redução das desigualdades sociais. Ensaio: Avaliação e Políticas Públicas em Educação, v. 25, n. 95, p. 393-413, 2017. Disponível em <<https://bit.ly/2mgJcK1>>. Acesso em 13 set. 2019.
- 100 *ibid.*
- 101 MICHAELIS. **Aliciar**. Disponível em: <<https://bit.ly/2mpFgGN>>. Acesso em: 12 set. 2019.
- 102 FUNDAÇÃO ABRINQ. **Pode ser abuso**. Disponível em <<https://bit.ly/2VpdM4G>>. Acesso em 17 set. 2019.
- 103 BRETAN, Maria Emília. **Violência sexual contra crianças e adolescentes mediada pela tecnologia da informação e comunicação**: elementos para a prevenção vitimal. 2012. Tese (Doutorado em Direito) - . Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012. p. 6. Disponível em <<https://bit.ly/2m2Tf56>>. Acesso em 19 set. 2019
- 104 *Idem.*
- 105 O'CONNELL, R. **A Typology of Child Cyber Sexploitation and On-line Grooming Practices**. Preston: Cyberspace Research Unit, University of Lancashire, 2003. Disponível em: <<https://bit.ly/2kVM7Yf>>. Acesso em: 19 set. 2019.
- 106 SAFERNET. **Início**. Disponível em <<https://bit.ly/2td2RdR>>. Acesso em 19 set. 2019.
- 107 MORAES, Mayra Lopes; AGUADO, Alexandre Garcia. **O uso da Internet para aliciamento sexual das crianças**. Revista Tecnológica da Fatec Americana, v. 2, n. 1, p. 23p.-23p., 2014. Disponível em <<https://bit.ly/2kIUHJW>>. Acesso em 19 set. 2019
- 108 MITNICK, D. K.; SIMON, L. W. Mitnick. **A arte de enganar**. Ataques de Hackers: controlando o fator humano na segurança da informação. Tradução: Kátia Aparecida Roque. São Paulo: Pearson, 1963
- 109 MANN, Lan. **Engenharia Social**: séries prevenção de fraudes. São Paulo: Blucher, 2011.
- 110 DA SILVA GERALDO, Vinicius; TAKEDA, Fábio Bento. **ENGENHARIA SOCIAL**. Revista Interface Tecnológica, v. 16, n. 1, p. 242-253, 2019. Disponível em <<https://bit.ly/2mptKeG>>. Acesso em 19 set. 2019
- 111 CERT. **Golpes na internet**. Disponível em <<https://bit.ly/2PeeSfv>>. Acesso em 19 set. 2019.
- 112 GAUCHAZH. **Phishing**: como evitar o golpe utilizado em 90% dos roubos de informações pessoais pela internet. Disponível em <<https://bit.ly/2mpfd2z>>. Acesso em 19 set. 2019.

- 113 CERT. **Golpes na internet**. Disponível em <<https://bit.ly/2PeeSfV>>. Acesso em 19 set. 2019.
- 114 CERT. **Cartilha de Segurança para Internet**. Disponível em <<https://bit.ly/2JBHjAe>>. Acesso em 30 out. 2019.
- 115 Coding Rights. **Manda nudes!** Disponível em <<https://bit.ly/2rdm2SK>>, acesso em 20 set. 2019.
- 116 ALEXY et al. **Perceptions of Cyberstalking Among College Students**. In: Brief Treatment and Crisis Intervention. Oxford University Press, 2005. 279-289. Disponível em: <<https://bit.ly/2m6qpRI>>. Acesso em 19 set. 2019.
- 117 BOCIJ, Paul; MCFARLANE, Leroy. **Online harassment: Towards a definition of cyberstalking**. Prison Service Journal, 139, 2002. 31-38. Disponível em: <<https://bit.ly/2knW6oO>>. Acesso em: 19 set. 2019.
- 118 BRASIL. **Decreto-Lei nº 3.688, de 3 de outubro de 1941**. Lei das Contravenções Penais. Disponível em: <<https://bit.ly/2OXNWkA>>. Acesso em: 19 set. 2019.
- 119 BRASIL. **Decreto-lei nº 2.848, de 7 de Dezembro de 1940** - Código Penal. Disponível em: <<http://bit.ly/2Pulbe2>>. Acesso em 29 out. 2019.
- 120 BRASIL. **Lei nº 13005, de 12 de junho de 2019**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, para incluir o art. 147-A, que dispõe sobre o crime de perseguição insidiosa ou obsessiva (stalking). Disponível em: <<https://bit.ly/2kvqptW>>. Acesso em: 19 set. 2019.
- 121 DE ABREU, Cristiano Ricardo Faedo Nabuco et al. **Dependência de Internet e de jogos eletrônicos: uma revisão**. Revista Brasileira de psiquiatria, v. 30, n. 2, 2008. Disponível em <<https://bit.ly/36MNmuV>>, acesso em 19 set. 2019.
- 122 Internet addiction, pathological internet use, internet addiction disorder, compulsive internet use, computer mediated communications addicts, computer junkies e internet dependency.
- 123 Ambulatório Integrado do Controle dos Impulsos / PRO-AMITI. **Dependência da internet**. Disponível em <<https://bit.ly/2m6ehjA>>, acesso em 19 set. 2019.
- 124 GCFglobal. **O que é controle parental?**. Disponível em <<https://bit.ly/2lWYn6a>>. Acesso em 19 set. 2019.
- 125 CARMO, Paloma; DUARTE, Felipe; GOMES, Ana Bárbara. **Glossário da Inclusão Digital - Volume I**. Instituto de Referência em Internet e Sociedade: Belo Horizonte, 2019. p. 48 Disponível em: <<https://bit.ly/33aGTJb>>. Acesso em: 30 out. 2019.
- 126 RESEARCH AND MARKETS. Global Computer Parental Control Market 2017-2025: Market is Expected to Reach \$3.3 Billion. Disponível em <<https://prn.to/2mqEhGs>>. Acesso em 19 set. 2019

- 127 MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. **Controle parental.** Disponível em <<https://bit.ly/2HV4UNo>>. Acesso em 20 set. 2019.
- 128 VALCKE, Martin et al. **Internet parenting styles and the impact on Internet use of primary school children.** Computers & Education, v. 55, n. 2, p. 454-464, 2010. Disponível em <<https://bit.ly/2msDdlq>>. Acesso em 20 set. 2019
- 129 BURATTO, Rafael Paiva; GLANZMANN, José Honório. **Controle Parental:** uma análise das principais ferramentas para monitoramento e controle dos filhos na Internet. Seminários de Trabalho de Conclusão de Curso do Bacharelado em Sistemas de Informação, v. 1, n. 1, 2016. Disponível em <<https://bit.ly/2m6Xcpp>>. Acesso em 20 set. 2019
- 130 NERIS, Natália; RUIZ, Juliana Pacetta; VALENTE, Mariana Giorgetti. **Análise comparada de estratégias de enfrentamento a “revenge porn” pelo mundo.** Rev. Bras. Polit. Públicas, Brasília, v. 7, nº 3, 2017 p. 333-347. Disponível em <<https://bit.ly/32AVaxu>>, acesso em 25 set 2019.
- 131 Ibidem. pag. 340.
- 132 CAPANEMA, Walter Aranha. **O direito ao anonimato:** uma nova interpretação do art. 5º, IV, CF. A voz do cidadão, 2017. Disponível em <<https://bit.ly/2kFKFZY>>. Acesso em 23 set. 2019.
- 133 MACHADO, Diego Carvalho. **Tutela jurídica da privacidade, anonimização de dados e anonimato na internet.** Tecnologias e conectividade [recurso eletrônico]: direito e políticas na governança das redes / Fabrício Bertini Pasquot Polido, Lucas Costa dos Anjos, Luiza Couto Chaves Brandão, organizadores. – Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2018. Disponível em <<https://bit.ly/2MWa3UB>>. Acesso em 23 set. 2019
- 134 Ibid, p. 273.
- 135 CAPANEMA, Walter Aranha. **O direito ao anonimato: uma nova interpretação do art. 5º, IV, CF.** A voz do cidadão, 2017. Disponível em <<https://bit.ly/2kFKFZY>>. Acesso em 23 set. 2019.
- 136 RECUERO, R. **Redes sociais na internet.** Porto Alegre: Sulina, 2010. p. 191.
- 137 WOLTON, D. **Internet, e depois?** Uma teoria crítica das novas mídias. 2. ed. Trad. bras. Isabel Crossetti. Porto Alegre: Sulina, 2007. p. 231.
- 138 CARVALHO, Thatyane Gama et al. **Elementos, finalidades e consequências da superexposição de usuários nas redes sociais.** Revista Científica de Comunicação Social do Centro Universitário de Belo Horizonte (unibh): e-Com, Belo Horizonte, v. 10, n. 2, p.16-30, jul. 2017. Semestral. Disponível em: <<https://bit.ly/34zOzEz>>. Acesso em: 10 out. 2019.
- 139 LIM, Weng Marc et al. **Overexposure in Social Networking Sites.** Journal

**Of Research For Consumers**, [s.i.], v. 22, p.25-40, jul. 2012. Semestral. Disponível em: <<https://bit.ly/35AilKP>>. Acesso em: 10 out. 2019.

<sup>140</sup> SAFERNET. **Vigilantismo**. Disponível em <<https://bit.ly/2kKXCSp>>, acesso em 17 de set. 2019.

<sup>141</sup> TROTTIER, Daniel. **Digital Vigilantism as Weaponisation of Visibility**. Philosophy & Technology, [s.l.], v. 30, n. 1, p.55-72, 1 abr. 2016. Springer Science and Business Media LLC. <http://dx.doi.org/10.1007/s13347-016-0216-4>. Disponível em: <<https://bit.ly/2mcTj8O>>. Acesso em: 19 set. 2019.

## AUTORIA

### ANA BÁRBARA GOMES

Pesquisadora do Instituto de Referência Internet e Sociedade. É graduanda em Ciências Sociais na UFMG. Foi bolsista do Programa de Ensino Tutoriado – PET Ciências Sociais, onde desenvolveu uma pesquisa sobre o uso de drones em operações militares e controvérsias sociotécnicas. Fez parte do Observatório de Inovação, Cidadania e Tecnociência (InCiTe-UFMG), integrando estudos sobre sociologia da ciência e tecnologia. Tem interesse nas áreas de governança algorítmica, vigilância, governança de dados e direitos humanos na internet.

### FELIPE MARCELO DUARTE

Estagiário de comunicação e pesquisador do Instituto de Referência Internet e Sociedade. Graduando em Comunicação Social na UFMG, desenvolve atividades voltadas a criação gráfica, audiovisual, ilustração e marketing. Trabalhou como diretor de arte na Cria UFMG e estagiário de comunicação na startup Bluelux. Tem interesse nas áreas de inclusão digital, usabilidade em ambientes digitais e Design Transmídia.

### PALOMA ROCILLO ROLIM DO CARMO

Pesquisadora do Instituto de Referência em Internet e Sociedade. Graduanda em Direito na Universidade Federal de Minas Gerais (UFMG). Monitora do Grupo de Estudos sobre Internet, Inovação e Propriedade Intelectual (GNET - UFMG). Participou como bolsista PIBIC do projeto de pesquisa que abarca temáticas do Direito Internacional Privado, Direitos Humanos e Novas Tecnologias e é desenvolvido na mesma Universidade.

## 8. BIBLIOGRAFIA



ALEX Y et al. **Perceptions of Cyberstalking Among College Students**. In: Brief Treatment and Crisis Intervention. Oxford University Press, 2005. 279-289. Disponível em: <<https://bit.ly/2m6qpRi>>. Acesso em 19 set. 2019.

Ambulatório Integrado do Controle dos Impulsos / PRO-AMITI. **Dependência da internet**. Disponível em <<https://bit.ly/2m6ehjA>>, acesso em 19 set. 2019.

ANDREJEVIC, Mark. Privacy, exploitation, and the digital enclosure. **Amsterdam LF**, v. 1, p. 47, 2008. Disponível em <<https://bit.ly/2m6QcsG>>. Acesso em 12 set. 2019.

ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS. **Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression**, Frank La Rue. Nova York: Onu, 2011. Disponível em: <<https://bit.ly/2wtUFbk>>. Acesso em: 23 set. 2019.

ATKIN, David J.; JEFFRES, Leo W.; NEUENDORF, Kimberly A. Understanding Internet adoption as telecommunications behavior. **Journal of Broadcasting & Electronic Media**, v. 42, n. 4, p. 475-490, 1998.

BESSI, Alessandro et al. Science vs conspiracy: Collective narratives in the age of misinformation. **PloS one**, v. 10, n. 2, p. e0118093, 2015. Disponível em <<https://bit.ly/2lMZ2vM>>. Acesso em 04 set. 2019.

BIONI, Bruno. **Proteção de dados pessoais: A função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. p. 94.

BOCIJ,Paul;MCFARLANE,Leroy. **Onlineharassment: Towards a definition of cyberstalking**. Prison Service Journal, 139, 2002. 31-38. Disponível em: <<https://bit.ly/2knW6oO>>. Acesso em: 19 set. 2019.

BRAGA, Julião et al. **O livro do IETF**. CGI. br, São Paulo, v. 1, 2014. Disponível em <<https://bit.ly/2kviJIb>>. Acesso em 20 set. 2019



BRASIL. **Portaria Interministerial nº 147**, de 31 de maio de 1995. Brasília, 31 maio 1995. Disponível em: <<https://bit.ly/2kRiY0p>>. Acesso em: 23 set. 2019.

BRASIL. **Decreto de 03 de abril de 2000**. Institui Grupo de Trabalho Interministerial para examinar e propor políticas, diretrizes e normas relacionadas com as novas formas eletrônicas de interação. Brasília, Disponível em: <<https://bit.ly/2OsU55t>>. Acesso em: 12 set. 2019.

BRASIL. **Decreto Nº 10.087, de 5 de novembro De 2019**. Declara a revogação, para os fins do disposto no art. 16 da Lei Complementar nº 95, de 26 de fevereiro de 1998, de decretos normativos. Brasília, Disponível em: <<https://bit.ly/35LihYN>>. Acesso em: 13 nov. 2019.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 14 ago. 2018. Disponível em: <<https://bit.ly/2LIYwGr>>. Acesso em: 23 set. 2019.

\_\_\_\_\_. **Constituição (1988)**. Constituição da República Federativa do Brasil de 05 de outubro de 1988. Brasília, Disponível em: <<https://bit.ly/1bJYlGL>>. Acesso em: 12 set. 2019.

\_\_\_\_\_. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, Disponível em: <<https://bit.ly/2LIYwGr>>. Acesso em: 10 set. 2019.

\_\_\_\_\_. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, Disponível em: <<https://bit.ly/1kxaoKm>>. Acesso em: 10 set. 2019.

\_\_\_\_\_. **Lei Nº 13.185, de 6 de novembro de 2015**. Institui o Programa de Combate à Intimidação Sistemática ( Bullying ). Disponível em: <<https://bit.ly/2PX1P0J>>. Acesso em: 13 nov. 2019.

\_\_\_\_\_. **Decreto-Lei nº 3.688, de 3 de outubro de 1941.** Lei das Contravenções Penais. Disponível em: <<https://bit.ly/2OXNWkA>>. Acesso em: 19 set. 2019.

\_\_\_\_\_. **Decreto-lei nº 2.848, de 7 de Dezembro de 1940 -** Código Penal. Disponível em: <<http://bit.ly/2Pulbe2>>. Acesso em 29 out. 2019.

\_\_\_\_\_. **Lei nº 13005**, de 12 de junho de 2019. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, para incluir o art. 147-A, que dispõe sobre o crime de perseguição insidiosa ou obsessiva (stalking). Disponível em: <<https://bit.ly/2kvqptW>>. Acesso em: 19 set. 2019.

BRETAN, Maria Emília. **Violência sexual contra crianças e adolescentes mediada pela tecnologia da informação e comunicação:** elementos para a prevenção vitimal. 2012. Tese (Doutorado em Direito) - Faculdade de Direito da Universidade de São Paulo, São Paulo, 2012. p. 6. Disponível em <<https://bit.ly/2m2Tf56>>. Acesso em 19 set. 2019

BRUGGER, Winfried. **Proibição ou proteção do discurso do ódio?** Algumas observações sobre o direito alemão e o americano. Trad. Maria Angela Jardim de Santa Cruz Oliveira. Revista de Direito Público, v. 15 n. 117, jan./mar. 2007, p. 118. Disponível em: <<https://bit.ly/2m9mZNQ>>. Acesso em: 10 set 2019.

BURATTO, Rafael Paiva; GLANZMANN, José Honório. Controle Parental: uma análise das principais ferramentas para monitoramento e controle dos filhos na Internet. **Seminários de Trabalho de Conclusão de Curso do Bacharelado em Sistemas de Informação**, v. 1, n. 1, 2016. Disponível em <<https://bit.ly/2m6Xcpp>>. Acesso em 20 set. 2019

CAPANEMA, Walter Aranha. O direito ao anonimato: uma nova interpretação do art. 5º, IV, CF. **A voz do cidadão**, 2017. Disponível em <<https://bit.ly/2kFKFZY>>. Acesso em 23 set. 2019.

CAPURRO, Rafael. **Digital Ethics**. Disponível em: <<https://bit.ly/2lOMzaL>>. Acesso em: 12 set. 2019.

CARVALHO, Thatyane Gama et al. Elementos, finalidades e consequências da superexposição de usuários nas redes sociais. **Revista Científica de Comunicação Social do Centro Universitário de Belo Horizonte (unibh): e-Com**, Belo Horizonte, v. 10, n. 2, p.16-30, jul. 2017. Semestral. Disponível em: <<https://bit.ly/34zOzEz>>. Acesso em: 10 out. 2019.

CARMO, Paloma; DUARTE, Felipe; GOMES, Ana Bárbara. **Glossário da Inclusão Digital**- Volume I. Instituto de Referência em Internet e Sociedade: Belo Horizonte, 2019. Disponível em: <<https://bit.ly/33aGTJb>>. Acesso em: 10 out. 2019.

CASTELLS, Manuel. **A era da informação: economia, sociedade e cultura**. In: A Sociedade em rede. São Paulo: Paz e Terra, 2000. v. 1. p. 107 a 118.

CERT. **Cartilha de Segurança para Internet**. Disponível em <<https://bit.ly/2JBHjAe>>. Acesso em 30 out. 2019.

\_\_\_\_\_. **Golpes na internet**. Disponível em <<https://bit.ly/2PeeSfV>>. Acesso em 19 set. 2019.

CETIC.br. **Pesquisas sobre o uso das Tecnologias de Informação e Comunicação - TIC Governo Eletrônico 2017**. Disponível em <<https://bit.ly/36SrxKL>>, acesso em 28 out. 2019.

\_\_\_\_\_. Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação. Disponível em <<https://bit.ly/2maNouB>>. Acesso em 26/08/2019.

CGI.BR. **Documentos da Cúpula Mundial sobre a Sociedade da Informação**. CGI. br, São Paulo, v. 1, 2014. Disponível em <<https://bit.ly/2Yh1TiM>>. Acesso em 20 set. 2019.

\_\_\_\_\_. **Sobre o CGI.br**. Disponível em <<https://bit.ly/2m7IazU>>. Acesso em 23 set. 2019

\_\_\_\_\_. **Resolução CGI.br/RES/2009/003/P**. Disponível em <<https://bit.ly/2m74biq>>. Acesso em 23 set. 2019.

CODING RIGHTS. **Manda nudes!** Disponível em <<https://bit.ly/2rdm2SK>>, acesso em 20 set. 2019.

CONSELHO EUROPEU. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. Estrasburgo, 1981. Disponível em: <<http://bit.ly/2EwEJsE>>. Acesso em: 20 nov. 2019.

DA SILVA, Ângela Carrancho. Educação e tecnologia: entre o discurso e a prática. **Ensaio: avaliação e políticas públicas em educação**, v. 19, n. 72, p. 527-554, 2011. Disponível em <<https://bit.ly/2mc1zj6>>. Acesso em 09 set. 2019

DA SILVA GERALDO, Vinicius; TAKEDA, Fábio Bento. ENGENHARIASOCIAL. **Revista Interface Tecnológica**, v. 16, n. 1, p. 242-253, 2019. Disponível em <<https://bit.ly/2mptKeG>>. Acesso em 19 set. 2019

DADVAR, Maral; DE JONG, Franciska. Cyberbullying detection: a step toward a safer internet yard. In: **Proceedings of the 21st International Conference on World Wide Web**. ACM, 2012. p. 121-126. Disponível em <<https://bit.ly/2kgm25L>>. Acesso em 02 ago. 2019.

DE ABREU, Cristiano Ricardo Faedo Nabuco et al. Dependência de Internet e de jogos eletrônicos: uma revisão. **Revista Brasileira de psiquiatria**, v. 30, n. 2, 2008. Disponível em <<https://bit.ly/36MNmuV>>, acesso em 19 set. 2019.

DE ALMEIDA FERREIRA, Norma Sandra. As pesquisas denominadas estado da arte. **Educação & sociedade**, v. 23, p. 257, 2002. Disponível em <<https://bit.ly/2Hyi5C2>>. Acesso em 12 de ago. de 2019

DE CASTRO, Julio Cesar Lemes. **O consumo na era da interpelação algorítmica**. Disponível em <<https://bit.ly/2pnqnXp>>. Acesso em 20 out. 2019

DIAS, Paulo. Comunidades de educação e inovação na sociedade digital. **Educação, Formação & Tecnologias-ISSN 1646-933X**, v. 5, n. 2, p. 4-10, 2012. Disponível em <<https://bit.ly/2kzafjm>>. Acesso em 13 set. 2019.

DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais**. Rio de Janeiro: Renovar, 2006. p.24

DUGGAN, Maeve. **Online harassment**. Pew Research Center, 2014. Disponível em <<https://pewrsr.ch/2kzia02>>. Acesso em 02 ago. 2019

ECHALAR, Adda Daniela Lima Figueiredo; PEIXOTO, Joana. Programa Um Computador por Aluno: o acesso às tecnologias digitais como estratégia para a redução das desigualdades sociais. **Ensaio: Avaliação e Políticas Públicas em Educação**, v. 25, n. 95, p. 393-413, 2017. Disponível em <<https://bit.ly/2lSWV9q>>. Acesso em 03 jul. 2019.

ESPELAGE, Dorothy L.; SWEARER NAPOLITANO, Susan M. **Research on school bullying and victimization: What have we learned and where do we go from here?**[Mini-series]. 2003 Disponível em <<https://bit.ly/2lTmzLg>>. 02 ago. 2019.

FANTIN, Monica. **“Nativos e imigrantes digitais” em questão: crianças e competências midiáticas na escola**. p.9. Passagens, Ceará, 2016. Disponível em: <<https://bit.ly/34D6dHs>>. Acesso em: 1 ago. 2019.

FUNDAÇÃO ABRINQ. **Pode ser abuso**. Disponível em <<https://bit.ly/2VpdM4G>>. Acesso em 17 set. 2019.

GAGLIARDONE, Iginio. “A country in order”: Technopolitics, nation building, and the development of ICT in Ethiopia. **Information Technologies & International Development**, v. 10, n. 1, p. pp. 3-19, 2014. Disponível em <<https://bit.ly/2m9qBzl>>. Acesso em 13 set. 2019

GAUCHAZH. **Phishing**: como evitar o golpe utilizado em 90% dos roubos de informações pessoais pela internet. Disponível

em <<https://bit.ly/2mpfd2z>>. Acesso em 19 set. 2019.

GAWER, Annabelle; CUSUMANO, Michael A. Industry platforms and ecosystem innovation. **Journal of product innovation management**, v. 31, n. 3, p. 417-433, 2014. Disponível em <<https://bit.ly/2kevcXj>>. Acesso em 11 set. 2019.

GCFglobal. **O que é controle parental?**. Disponível em <<https://bit.ly/2lWyN6a>>. Acesso em 19 set. 2019.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. Editora Atlas SA, 2008. Disponível em <<https://bit.ly/2kMjLiU>>. Acesso em 16 set. 2019.

HAMELINK, Cees J. **The ethics of cyberspace**. Sage, 2000. Disponível em <<https://bit.ly/2m95U6B>>. Acesso em 12 set. 2019.

HARRIS, Brent. **Establishing Structure and Governance for an Independent Oversight Board**. Disponível em <<https://bit.ly/2mlgY0H>>. Acesso em 22 out. 2019.

HAYLES, N. Katherine. Hyper and deep attention: The generational divide in cognitive modes. **Profession**, v. 2007, n. 1, p. 187-199, 2007. Disponível em <<https://bit.ly/2ELiGA9>>. Acesso em 09 set. 2019.

HENRY, Daniel. **Media and the Law**. Disponível em <<https://bit.ly/2lN8lMe>>. Acesso em 13 set. 2019

HOWELL, Lee et al. Digital wildfires in a hyperconnected world. **WEF report**, v. 3, p. 15-94, 2013.

INTERVOZES. **Contribuições para uma regulação democrática das grandes plataformas que garanta a liberdade de expressão na internet**: Uma perspectiva latino-americana para alcançar processos de moderação de conteúdo compatíveis com os padrões internacionais de direitos humanos. Disponível em: <<https://bit.ly/2kfRYHp>>. Acesso em: 22 out. 2019.

IRETON, Cherilyn; POSETTI, Julie (Org.). **Jornalismo, Fake News & Desinformação: Manual para Educação e Treinamento em Jornalismo**. Paris: Organização das Nações Unidas Para A Educação, A Ciência e A Cultura (unesco)., 2019. 129 p. Tradução de Sarah Rebouças Reedman. Disponível em: <<https://bit.ly/2MWUON0>>. Acesso em: 03 set. 2019.

IRIS. **Representação ao Ministério Público de Minas Gerais - MPMG**. 2018. Disponível em: <<http://bit.ly/32Z4cp1>>. Acesso em 29 out. 2019.

\_\_\_\_\_. **Projeto de Pesquisa Barreiras e Desafios à inclusão digital no Brasil: Instrumentos do Direito & Tecnologias Para Transformação da Realidade Social Digital**. Disponível em <<https://bit.ly/342Pe2p>>, acesso em 28 de ago. de 2019.

KAPLAN, Andreas M. HAENLEIN, Michael. **Users of the world, unite! The challenges and opportunities of Social Media**. *Business Horizons*, Estados Unidos, 53, p.59-68, 2010. Disponível em: <<https://bit.ly/2YWtNwU>>. Acesso em 06 set. 2019.

KUENZER, Acácia Zeneida. Da dualidade assumida à dualidade negada: o discurso da flexibilização justifica a inclusão excludente. **Educação & Sociedade**, v. 28, n. 100, p. 1153-1178, 2007. Disponível em <<https://bit.ly/2kKaFDs>>. Acesso em 13 set. 2019.

KUNER, C., CATE, F. H., MILLARD, C., e SVANTESSON, D. J. B. Privacy—an elusive concept. **International Data Privacy Law**, 1(3), 2011. p. 141-142.

KURBALIJA, Jovan. **Uma introdução à governança da internet**. São Paulo: Comitê Gestor da Internet no Brasil, 2016. Disponível em <<https://bit.ly/2w8OQ2r>>. Acesso em 20 set. 2019

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2011.

\_\_\_\_\_. **Responsabilidade Civil dos Provedores de Serviços**

**de Internet.** Disponível em: <<https://bit.ly/2kkOMKO>>. Acesso em 06 set. 2019.

LEWIS, Paul. 2018. **'Fiction is outperforming reality':** how YouTube's algorithm distorts truth. The Guardian, Fevereiro, 2018. Disponível em <<http://bit.ly/2EqBq8p>> acesso em 12 set. 2019.

LIM, Weng Marc et al. Overexposure in Social Networking Sites. **Journal Of Research For Consumers**, [s.i.], v. 22, p.25-40, jul. 2012. Semestral. Disponível em: <<https://bit.ly/35AilKP>>. Acesso em: 10 out. 2019.

LOUREIRO, Carla Cristiane; GRIMM, Viviane; LUNARDI-MENDES, Geovana M. **“Imigrantes” versus “nativos” digitais:** O discurso de tecnologias digitais em políticas curriculares. **Roteiro**, v. 41, n. 3, p. 731, 2016. Disponível em <<https://bit.ly/2lMufz4>>

MACHADO, Diego Carvalho. Tutela jurídica da privacidade, anonimização de dados e anonimato na internet. **Tecnologias e conectividade [recurso eletrônico]: direito e políticas na governança das redes** / Fabrício Bertini Pasquot Polido, Lucas Costa dos Anjos, Luiza Couto Chaves Brandão, organizadores. – Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2018. Disponível em <<https://bit.ly/2MWa3UB>>. Acesso em 23 set. 2019

MANN, Lan. **Engenharia Social:** séries prevenção de fraudes. São Paulo: Blucher, 2011.

MICHAELIS. **Aliciar.** Disponível em: <<https://bit.ly/2mpFgGN>>. Acesso em: 12 set. 2019.

\_\_\_\_\_. **Digital.** Disponível em: <<https://bit.ly/2kxxTg8>>. Acesso em: 12 set. 2019.

MINISTÉRIO DA ECONOMIA. **Governo Eletrônico.** Disponível em: <<https://bit.ly/2khUddd>>. Acesso em: 12 set. 2019.



MINISTÉRIO DA EDUCAÇÃO. **Programa um computador por aluno (PROUCA)**. Disponível em <<https://bit.ly/2Lrxo0z>>. Acesso em 13 set. 2019

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. **Controle parental**. Disponível em <<https://bit.ly/2HV4UNo>>. Acesso em 20 set. 2019.

MITCHELL, Kimberly J. et al. What features make online harassment incidents upsetting to youth?. **Journal of school violence**, v. 15, n. 3, p. 279-301, 2016. Disponível em <<https://bit.ly/2lSHKNS>>. Acesso em 02 ago. 2019

MITNICK, D. K.; SIMON, L. W. Mitnick **A arte de enganar. Ataques de Hackers: controlando o fator humano na segurança da informação**. Tradução: Kátia Aparecida Roque. São Paulo: Pearson, 1963

MORAES, Mayra Lopes; AGUADO, Alexandre Garcia. O uso da Internet para aliciamento sexual das crianças. **Revista Tecnológica da Fatec Americana**, v. 2, n. 1, p. 23p.-23p., 2014. Disponível em <<https://bit.ly/2kIUHJW>>. Acesso em 19 set. 2019

MORI, Cristina Kiomi. **Políticas públicas para inclusão digital no Brasil: aspectos institucionais e efetividade de iniciativas federais de disseminação de telecentros no período 2000-2010**, (2011). Disponível em <<https://bit.ly/2maPF97>>. Acesso em 10 set. 2019.

NERIS, Natália; RUIZ, Juliana Pacetta; VALENTE, Mariana Giorgetti. Análise comparada de estratégias de enfrentamento a “revenge porn” pelo mundo. **Rev. Bras. Polít. Públicas**, Brasília, v. 7, nº 3, 2017 p. 333-347. Disponível em <<https://bit.ly/32AVaxu>>, acesso em 25 set 2019.

NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), **Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nos domicílios brasileiros - TIC Domicílios 2018**. Disponível em <<https://bit.ly/330YvHe>>, acesso em 09 set. 2019.

O'CONNELL, R. A Typology of Child Cyber Sexploitation and On-line Grooming Practices. Preston: **Cyberspace Research Unit**, University of Lancashire, 2003. Disponível em: <<https://bit.ly/2kVM7Yf>>. Acesso em: 19 set. 2019.

**O'REILLY**, Tim. **Web 2.0 Compact Definition: Trying Again**. Disponível em <<https://bit.ly/NIA49S>>. Acesso em 27 ago. 2019.

PALFREY, John; GASSER, Urs. **Nascidos na era digital: entendendo a primeira geração de nativos digitais**. Penso Editora, 2011. p. 31. Disponível em <<https://bit.ly/2kJKGvI>>. Acesso em 1 set. 2019

PASCOTTO, Alan. **Quais são os tipos de plataforma de e-commerce?**. Disponível em <<https://bit.ly/2m9Gmq3>>. Acesso em 23 set. 2019.

PATER-**Characterization of Online Harassment: Comparing Policies Across Social Media Platforms**. Disponível em <<https://bit.ly/2klrwwg>>. Acesso em 02 de ago. 2019.

PEREIRA, Marcus Abílio. **Internet e mobilização política - os movimentos sociais na era digital**. In: IV Encontro da Compolítica, 2011, Rio de Janeiro. Anais do IV Encontro da Associação Brasileira de Pesquisadores em Comunicação e Política, 2011. p. 1 - 26. Disponível em: <<https://bit.ly/35CEJ65>>. Acesso em: 28 out. 2019.

POLIDO, Fabrício, et al. **GDPR e suas repercussões no direito brasileiro: primeiras impressões de análise comparativa**. Instituto de Referência em Internet e Sociedade: Belo Horizonte, 208. Disponível em: <<https://bit.ly/2BEcG8W>>. Acesso em: 23 de out. de 2019.

PONTE, Cristina; SIMÕES, José Alberto. Comparando resultados sobre acessos e usos da internet: Brasil, Portugal e Europa. **Comitê Gestor da Internet no Brasil – CGI. BR. TIC Kids Online Brasil**, p. 27-35, 2012.

POSTER, Mark. **CyberDemocracy: Internet and the Public Sphere**. Disponível em <<https://bit.ly/2kTjQ4G>>. Acesso em 23 ago. 2018

PRENSKY, Marc. **Digital Natives, Digital Immigrants**. On the Horizon, Vol. 9 No. 5, NCB University Press, 2001. Disponível em: <<https://bit.ly/2ySL1ib>>. Acesso em: 1 ago. 2019.

PRIMO, A. O aspecto relacional das interações na Web 2.0. **E-Compós**, Brasília, v.9, p.1-21, 2007. Disponível em <<https://bit.ly/2m8y29Y>>. Acesso em 13 set. 2019.

RECUERO, R. **Redes sociais na internet**. Porto Alegre: Sulina, 2010. p. 191.

RESEARCH AND MARKETS. **Global Computer Parental Control Market 2017-2025: Market is Expected to Reach \$3.3 Billion**. Disponível em <<https://prn.to/2mqEhGs>>. Acesso em 19 set. 2019

RIBEIRO, Manoel Horta et al. **Auditing Radicalization Pathways on YouTube**. 2019. Disponível em: <<https://arxiv.org/abs/1908.08313>>. Acesso em: 28 nov. 2019.

ROGERS, Everett. Informatization, globalization, and privatization in the new Millenium. **Asian Journal of Communication**, v. 10, n. 2, p. 71-92, 2000. Disponível em <<https://bit.ly/2kGTQJx>>. Acesso em 12 set. 2019.

SACKMANN, Reinhold; WEYMANN, Ansgar. **Dietechnisierung des alltags: Generationen und technische innovationen**. Campus-Verlag, 1994. Disponível em <<https://bit.ly/2kjE4Eo>>. Acesso em 09 jul. 2019.

SAFERNET. **Início**. Disponível em <<https://bit.ly/2td2RdR>>. Acesso em 19 set. 2019.

\_\_\_\_\_. **Hotline**. Disponível em <<https://bit.ly/2zYwmo5>>. Acesso em 22 out. 2019

\_\_\_\_\_. **Vigilantismo..** Disponível em <<https://bit.ly/2kKXCSp>>, acesso em 17 set. 2019.

SALTARELLI, Bia. **Plataformas digitais:** o que é e como as grandes empresas do mundo utilizam? Disponível em: <<https://bit.ly/2kxyi28>>. Acesso em: 12 set. 2019.

SHIEBER, Jonathan. **Australia passes law to hold social media companies responsible for “abhorrent violent material”.** Disponível em <<https://tcn.ch/2uQS22e>>. Acesso em 13 set. 2019.

SILENCE, Elizabeth; BABER, Chris. Integrated digital communities: combining web-based interaction with text messaging to develop a system for encouraging group communication and competition. **Interacting with computers**, v. 16, n. 1, p. 93-113, 2004. Disponível em <<https://bit.ly/2IKTsKn>>. Acesso em 12 set. 2019.

SILVA, Bento Duarte da; PEREIRA, Maria da Graça Caridade Barbosa. O papel da escola no combate à divisão digital. In: **XI Congresso Luso Afro Brasileiro de Ciências Sociais: diversidades e (des) igualdades.** Universidade Federal da Bahia (UFBA), 2011. Disponível em <<https://bit.ly/2kK9DY6>>. Acesso em 06 set. 2019.

SILVA, Rosane L; NICHEL, Andressa; MARTINS, Anna C. L; BORCHARDT, Carlise K. **Discursos de ódio em redes sociais:** jurisprudência brasileira. Rev. direito GV [online]. 2011, vol.7, n.2, p. 445-468. Disponível em: <<https://bit.ly/2m8A7CO>>. Acesso em: 10 set. 2019.

SOLOVE, Daniel. **Understanding privacy.** Harvard University Press, 2010.

TERRA. **Anos 90:** o desenvolvimento da internet no Brasil. Disponível em: <<https://bit.ly/2IRIUZE>>. Acesso em: 12 set. 2019.

TROTTIER, Daniel. Digital Vigilantism as Weaponisation of

Visibility. **Philosophy & Technology**, [s.l.], v. 30, n. 1, p.55-72, 1 abr. 2016. Springer Science and Business Media LLC. <http://dx.doi.org/10.1007/s13347-016-0216-4>. Disponível em: <<https://bit.ly/2mcTJ8O>>. Acesso em: 19 set. 2019.

UNIÃO EUROPEIA. **Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho**, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE

(Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, Estrasburgo, 04/05/2016. Disponível em: <<https://bit.ly/2S2WGH7>>. Acesso em: 20 nov. 2019.

VALCKE, Martin et al. Internet parenting styles and the impact on Internet use of primary school children. **Computers & Education**, v.55, n. 2, p.454-464, 2010. Disponível em <<https://bit.ly/2msDdlq>>. Acesso em 20 set. 2019

VIEIRA, Victor B. R.; CORASSA, Eugênio D. **A importância da proteção de dados pessoais como direito fundamental**. Disponível em <<https://bit.ly/2kjIICk>>. Acesso em set. 2019.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy, **in 4 Harvard Law Review** **193**, 1890.

WELSCH, Wolfgang. Transculturality: The puzzling form of cultures today. **Spaces of culture: City, nation, world**, v. 13, n. 7, p.194-213, 1999. Disponível em <<https://bit.ly/2m9qMdZ>>. Acesso em 23 ago. 2019.

WERTHEIN, Jorge. A sociedade da informação e seus desafios. **Ci. Inf., Brasília**, v. 29, n. 2, p. 71-77, 2000. Disponível em <<https://bit.ly/2lWfmdK>>. Acesso em 16 set. 2019

WINNER, Langdon. Do artifacts have politics?. **Daedalus**, p. 121-136, 1980. Disponível em <<https://bit.ly/2TuKEXZ>>, acesso em 19/08/2019.

WOLTON, D. **Internet, e depois?** Uma teoria crítica das novas mídias. 2. ed. Trad. bras. Isabel Crossetti. Porto Alegre: Sulina, 2007. p. 231.

YOUTUBE. **Policies and Safety**. Disponível em <<https://bit.ly/2kOdmUv>>. Acesso em 17 set. 2019.

ZITTRAIN, Jonathan. **Privacy 2.0**. University of Chicago Legal Forum. 2008. Pag 65. Disponível em <<http://bit.ly/2sFwHuC>>, acesso em 11 dez. 2019.

ZUBOFF, S. Bigother: Surveillance capitalism and the prospects of an information civilization. **Journal of Information Technology**, v.30, n.1. p. 75-89. 2015.

iris