Desenho: Ernani Calazans

GUIA DE ESTUDOS

AGNU

Governabilidade algorítmica, coleta de dados e privacidade nas redes

ALEX LARA MARTINS

THIAGO BICALHO FERREIRA E ORIENTANDOS (EDIVAN DE SOUZA, ROBERTA CHAVES, THAINAN GOMES)

IFMUNDO 2019

Simulação da ONU no Instituto Federal do Norte de Minas Gerais

Sumário

Resumo da Simulação

Organismo: Assembleia Geral das Nações Unidas (AGNU)

Tema de debate: *Governabilidade Algorítmica, coleta de dados e privacidade nas redes*. Matéria encaminhada pelo Conselho de Direitos Humanos e Conselho de Segurança das Nações Unidas.

Motivo: Discutir, deliberar, recomendar, instituir e aprovar o regulamento internacional sobre a responsabilidade dos governos acerca da coleta, uso e segurança de dados na internet.

Quórum para aprovação: Questões simples = ½ + 1 dos presentes / Aprovação de Propostas = ⅔ das nações presentes votantes. Obs.: Neste comitê, apenas nações têm direito a voto para aprovação de propostas.

Nações, entidades e pessoas convocadas: **Obrigatórios**: Arábia Saudita, Argentina, Brasil, Bulgária, Canadá, China, Dinamarca, Estados unidos, França, Israel, Jordânia, Líbano, Reino Unido, Síria, Rússia, **Adicionais:** Alemanha, Emirados Árabes, Noruega, Etiópia, Índia, Irã, Iraque, Itália, Japão, Sudão, México, Nigéria, Polônia, Romênia, Turquia, Egito. **Especiais***: Edward Snowden, Anonymous, Facebook, Google.

*Membros Observadores: possuem direito a fala, mas não votam as propostas de resolução.

Introdução

O autor de ficção científica George Orwell descreve, no romance *1984*, um mundo em que os indivíduos são constantemente monitorados por televisores, que servem para propagar as ideias do governo ("o Grande Irmão – *Big Brother* – está de olho em você") e controlar o comportamento, os corpos e os pensamentos dos telespectadores. Esta distopia possui algumas semelhanças com a penitenciária idealizada pelo filósofo Jeremy Bentham: o panóptico. Estruturada de forma circular, gradeada, contendo uma torre de vigilância no meio, esta prisão requer um número mínimo de vigilantes, que observam os presos sem serem observados. O que a distopia de Orwell e a ideia de Bentham têm em comum? Em primeiro lugar, elas evocam dispositivos tecnológicos de comunicação e informação que permitem controlar e disciplinar os indivíduos. Esses dispositivos de controle possuem uma racionalidade própria, cada vez mais avançada, tecnicista e autônoma. Em segundo lugar, há uma relação desigual entre o observador e os sujeitos observados. O observador detém as informações e pode utilizá-las para ordenar o seu mundo fechado. Os sujeitos observados ignoram como as informações estão sendo

Google (2016) mostra que as pessoas subestimam ou ignoram a quantidade de vezes que são filmadas por uma câmera de segurança. Diariamente, a imagem de um londrino é capturada mais de 300 vezes. Um cidadão norte-americano é filmado cerca de 75 vezes por dia, embora tenha a impressão de ter sido vigiado por 10 vezes menos câmeras.

coletadas e para que elas são utilizadas. O Grande Irmão e o vigilante na torre da prisão são figuras abstratas, tais como o "sistema capitalista", o "sistema socialista", o "sistema globalista", o "sistema dominante", o "sistema opressor", o "sistema burocrático", o "sistema informatizado" etc. Essas figuras de "sistema" sequer precisam ter existência real: basta que os sujeitos observados acreditem nelas. Em terceiro lugar, os sistemas de controle disciplinar ocorrem em ambientes relativamente fechados em que os indivíduos não são livres para acessarem o ambiente externo. Nos ambientes de confinamento, os corpos se tornam dóceis e os comportamentos se amoldam com facilidade, os sujeitos se sentem muito seguros, há pouca possibilidade para os crimes comuns, existe cumplicidade, solidariedade e harmonia dentro do grupo social. Neste caso, o preço da segurança absoluta é a completa escassez da liberdade. Estaríamos mais próximos de um episódio de Black Mirror (ver os episódios *White Christmas* e *The Entire History of You*) do que de um sistema político opressor como o descrito por Orwell.

A liberdade, a segurança e a vida compõem os direitos humanos fundamentais dos indivíduos, previstos no 3º artigo da Declaração Universal dos Direitos Humanos. Este artigo tem relações estreitas com os artigos 5 (dever ao tratamento humanizado), 9 (contra a arbitrariedade da prisão) e, principalmente, o 12 (direito à privacidade). Em conjunto, os artigos protegem os Direitos Individuais e os colocam acima dos Direitos do Estado. Este não teria permissão para subtrair do indivíduo qualquer item que venha a diminuir a sua dignidade e os seus direitos básicos de vida e liberdade:

> Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra essas intromissões ou ataques toda a pessoa tem direito a proteção da lei (ONU, 1948, §12).

A privacidade é um valor humano que permite o desenvolvimento de uma personalidade sem interferências externas não consentidas. A privacidade nos permite estabelecer as fronteiras entre nós mesmos e os outros. Ela limita o acesso dos outros aos nossos corpos, lugares, coisas e informações, de modo que os nossos desejos, crenças e pensamentos possam se manifestar livremente, sem opressão (ONUBR, 2018). Em casos extremos, no entanto, a manutenção da privacidade pode colocar em risco outros direitos fundamentais do indivíduo e da coletividade.

Há casos em que a liberdade de expressão é invocada para justificar ofensas a grupos e minorias, sem que haja a identificação de autoria. Os criminosos cibernéticos buscam formas de esconderem-se na rede, subvertendo, algumas vezes, o princípio da privacidade. Este mesmo princípio pode impedir que autoridades obtenham informações relevantes para algumas investigações criminais. Esses exemplos podem justificar a intromissão e o desrespeito à privacidade? Pode o Estado intervir e acessar as informações de uma pessoa com o objetivo de resguardar a vida e a segurança dos demais? Se

o direito à privacidade é apenas limitante, mas não totalmente impeditivo, quais critérios devemos utilizar para estabelecer até onde vai o controle externo, estatal, policial ou de outra natureza? A simulação desta sessão especial da Assembleia Geral das Nações Unidas pretende estabelecer estes limites à responsabilidade dos diferentes governos sobre as informações de seus cidadãos. Espera-se que estes limites sejam debatidos e acordados em um regulamento internacional sobre o acesso e o uso de informações pessoais na rede mundial de computadores. Chamaremos este documento de **RGDP.ONU**. Durante a simulação, os delegados devem estar atentos aos seguintes eixos para confecção deste regulamento: a Privacidade; a Neutralidade; a Inimputabilidade; e a Segurança nas redes (ver Seção 1.4).

RGDP é o termo acadêmico para o Regulamento Geral de Proteção dos Dados Pessoais. A sigla em inglês é GDPR (*General Data Protection Regulation*). Após a sigla indica-se a abrangência do Regulamento.
A proposta deste comitê consiste na no debate para a criação do RGDP.ONU.

A Assembleia Geral é o local adequado para o estabelecimento deste tipo de compromisso. Este é um dos principais organismos da ONU. A AGNU possui órgãos subsidiários, tais como a Comissão de Direito Internacional e o Conselho de Direitos Humanos, além de estabelecer as diretrizes para programas e fundos internacionais, tais como as Conferências das Nações Unidas sobre o Comércio e o desenvolvimento. Em geral, a Assembleia é demandada em questões críticas que envolvem múltiplos atores. As suas principais atribuições têm a ver com a supervisão e orientação dos trabalhos dos outros órgãos, bem como a expedição de recomendações e resoluções diversas. Trata-se de uma plataforma ampliada para debates que pressupõe a representação igualitária, ou seja, nela os países membros têm poderes iguais de voz e voto. A Assembleia Geral é comandada pelo Secretário Geral em sessões anuais regulares ou em sessões especiais (como é o caso desta proposta de simulação). O Capítulo IV da Carta das Nações Unidas estabelece as suas atribuições e regulamenta os procedimentos da AGNU.

As moções importantes da AGNU – como as recomendações relacionadas à segurança mundial, as questões orçamentárias e a composição da Assembleia – necessitam de maioria absoluta para serem aprovadas, ou seja, de pelo menos dois terços dos membros presentes e votantes. As demais questões são decididas por maioria simples. Os votos de cada país membro possuem igualdade de peso. É importante salientar que resoluções da Assembleia não são vinculantes, mantendo-se como recomendativas. Por outro lado, dentro de sua autonomia jurídica, os países membros podem assumir compromissos e se basear nas recomendações para criar uma jurisdição própria. As recomendações da AGNU, no âmbito das Nações Unidas, quase nunca se referem à segurança, que é responsabilidade do Conselho de Segurança. Para fins da simulação proposta, no entanto, devemos assumir que tanto o Conselho de Segurança quanto o Conselho de Direitos Humanos provocaram a AGNU para que se estabeleça em seus domínios as diretrizes governamentais de segurança em rede que respeitem as normas dos Direitos Humanos.

Embora o objetivo deste comitê seja a construção coletiva de um regulamento jurídico

recomendativo, as questões a serem debatidas são mais amplas do que as do Direito e das legislações nacionais (as regras estabelecidas por cada país). Isso porque a governabilidade algorítmica surge como uma nova forma de administração do poder, que não pressupõe apenas a racionalidade humana, como também os cálculos automatizados para as tomadas de decisão políticas e controle da população. Por isso, incentivamos os delegados a buscarem outras perspectivas de análise, que podem envolver o estudo sobre o funcionamento das novas tecnologias e sobre como elas afetam os indivíduos na sociedade atual. Os avanços tecnológicos nas áreas de controle da informação e de segurança no ambiente virtual trazem à tona reflexões de ordem econômica, política e ética. A seguir, apresentamos todas essas questões em conjunto: as definições e conceitos técnicos relevantes; os aspectos legais, éticos e socioculturais em torno do tema; onde e quando o problema surgiu; e qual a importância de resolvê-lo em âmbito mundial.

1 Apresentação do Tema: perspectivas éticas, políticas e tecnológicas

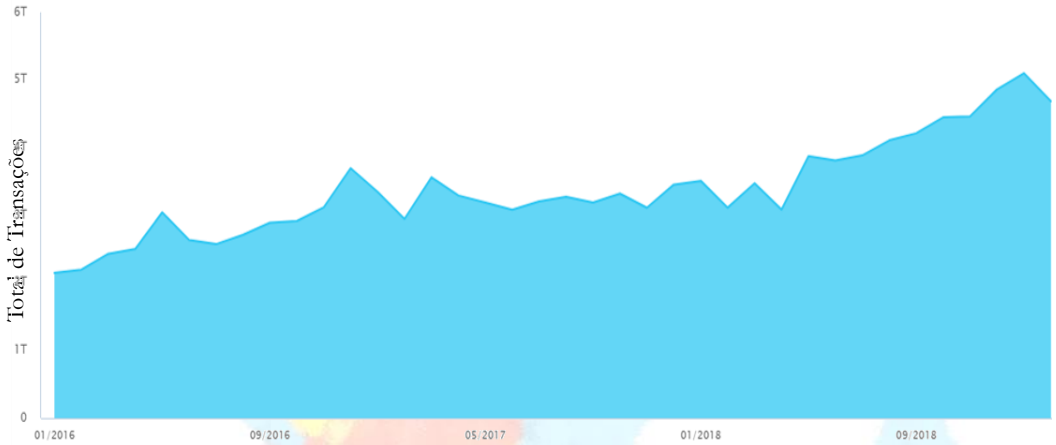
As novas formas de relação social estão ligadas ou mediadas pelo ambiente digital denominado **ciberespaço**, cujo acesso é realizado via internet (ALVES, 2016, p. 497). Chama atenção a crescente interação entre os seres humanos e máquinas. Estas são capazes de receber, arquivar e transmitir informações de caráter pessoal. Avalia-se que até 2030 as tecnologias de inteligência artificial regularão as áreas de transporte, serviços caseiros, saúde, educação, grupos comunitários, segurança pública, emprego e entretenimento (STONE et al., 2016). As tecnologias de monitoramento com inteligência artificial podem causar preocupação quando utilizadas de modo irresponsável, ou melhor, quando não resguardam o espírito da Declaração Universal dos Direitos Humanos (1948), documento que pretendeu estabelecer os princípios gerais entre os povos, tais como a paz, a liberdade, a igualdade, a dignidade e o progresso. O artigo 12º dessa carta institui que

> Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra essas intromissões ou ataques toda a pessoa tem direito a proteção da lei.

Isso significa que a privacidade é um direito fundamental do ser humano. Na era digital em que vivemos, mediada pelo acesso à internet, as informações pessoais são armazenadas em bancos de dados aos quais, muitas vezes, o próprio usuário não possui acesso direto, como se os seus traços digitais não lhes pertencessem. O uso de novas tecnologias e o avanço do conhecimento sobre dispositivos de processamento e de comunicação ilustram o que o sociólogo Manuel Castells (1999, p. 69) denomina de quarta revolução tecnológica, em que a própria sociedade se estabelece no cibercespaço ou ambiente de rede. Embora a criação de grandes bancos de dados facilite o acesso do usuário à rede e, por conseguinte, permita as suas ações sociais, a lógica deste novo sistema tecnológico pode ser utilizada para o controle

das massas. Com o avanço das tecnologias e a ampliação dos meios de comunicação, o fluxo de informações tem aumentado exponencialmente (Gráf. 1). Cada vez mais, as pessoas compartilham aspectos da sua vida na internet, em especial, nas redes sociais. Depositam informações pessoais e alimentam bancos de dados economicamente valiosos.

Gráfico 1: Tráfego na internet (2016-2019)



Este gráfico destaca como o tráfego geral (solicitações e respostas) mudou entre **janeiro de 2016 e fevereiro de 2019**. No geral, o volume de tráfego nos servidores DNS em todo o mundo **aumentou em 54%** nesse período de tempo.

Fonte: AKAMAI TECH, 2019.

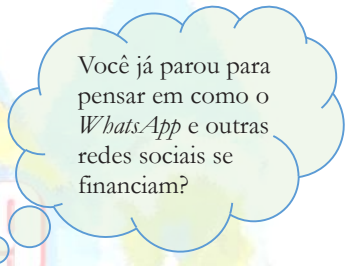
O que eu e você pensamos e sentimos? De que gostamos e necessitamos? Para onde vamos todos os dias? O que discutimos em casa e na escola e a quais conclusões chegamos? Como nos comportamos diante das diferentes circunstâncias? Tudo isso pode ser bastante relativo e não ter grande valor, a não ser que se estabeleçam padrões que relacionem todas esses dados e metadados, transformando-os em informação e conhecimento rentável. É isto o que fazem os algoritmos: programam as máquinas para receberem e tratarem o conjunto de dados, cujo resultado oferece um padrão comportamental. Cidades como Pequim, na China, possuem cerca de meio bilhão de câmeras, muitas das quais possuem tecnologia de reconhecimento facial que permite ao centro de controle encontrar um cidadão em menos de 10 minutos (LIU, 2017). Existem possibilidades ainda mais radicais de monitoramento, como **o uso de microchips sob a pele**. O objetivo dessas tecnologias é tanto prevenir quanto prever o comportamento criminoso. A lógica por detrás da aceitação dessas tecnologias é: "se você não tem nada para esconder, você não tem do que temer".

O uso de microchips em seres humanos foi um dos temas de debate do IFMUNDO 2018. Os documentos produzidos estão disponíveis em https://ifmundo.wordpress.com/comites/acnudh/

Sensores nos mais diferentes lugares podem permitir o rastreamento completo das atividades de uma pessoa. Essa tecnologia possibilita desenvolver um verdadeiro e completo sistema de vigilância, a ser utilizado pelas mais diversas instituições (policiais, militares, médicas, comerciais, industriais etc.), criando uma atmosfera de vigilância e monitoramento, que é a base da sociedade de controle preconizada pelo filósofo Gilles Deleuze:

> coleiras eletrônicas capazes de detectar a posição de cada indivíduo, lícita ou ilicitamente, operando uma modulação universal, seriam os novos instrumentos de controle a serem implantados no lugar dos meios de confinamento disciplinares estudados por Foucault. É a sociedade de controle substituindo a sociedade disciplinar (DELEUZE, 1992, p. 220).

As sociedades de controle substituíram as sociedades disciplinares dos séculos XIX e XX, que se organizavam por meio de instituições de confinamento: a escola, o hospital, a caserna, a fábrica. Na sociedade do século XXI, porém, os espaços sociais fechados são substituídos por circuitos abertos e sem fronteiras, como é o caso da internet. Os mecanismos de controle, segundo Deleuze, tendem a ser adaptados a esse novo contexto. Estaríamos vivenciando o novo panóptico ou panóptico digital (ALVES, 2016, p. 494). Pelo simples cruzamento de dados de localização, é possível extrair conclusões a respeito do comportamento de uma pessoa, por exemplo, os locais que frequenta, o horário, o tempo que permanece ali, com quem pode ter conversado e quais foram os tópicos da conversa (supondo que as pessoas tenham utilizado buscadores na internet).



Se a simples possibilidade de monitoramento dos deslocamentos de uma pessoa já causa preocupação, o que se dizer dessa funcionalidade atrelada à possibilidade de acesso automático a dados sensíveis da pessoa monitorada? Outro questionamento importante é saber a quem pertencem os dados coletados: da pessoa que aceita os termos de uso ou da empresa que disponibiliza o *software* ao usuário? Esta última pode exercer o monitoramento da vida de uma pessoa, através dos dados sobre a identidade e o comportamento, acessando muitas outras informações que ficam disponíveis na sua base de dados. E não é apenas o acesso ao número de informações que preocupa. Esses dados podem ser processados por sistemas mantidos pelas empresas que desenvolvem o programa, produzindo informações relevantes de alto valor comercial. A internet se transformou numa indústria multibilionária e empresas como *Google* e *Facebook* possuem enorme estoque de informações pessoais que podem ser utilizadas comercialmente e para fins políticos, o que pode, inclusive, ser uma ameaça à democracia.

Defensores dos Direitos Humanos exigem que essa tecnologia deva ser imediatamente regulamentada, estabelecendo-se **limites** no acesso das informações e definindo-se responsabilidades e obrigações de segurança dos dados para os mantenedores do sistema. Entre as obrigações, devem também ser incluídas cláusulas de segurança dos dados para empresas que operam a tecnologia, contendo detalhes de segurança contra acessos não autorizados (ataques *hackers*), bem como a instauração de conselhos internos de ética para avaliação do desenvolvimento de tecnologias de inteligência artificial em áreas de vigilância e análise de dados. Diversos países seguem o preceito internacional de que "a vida privada da pessoa é inviolável". Por outro lado, deve-se considerar que esse tipo de tecnologia pode trazer

resultados benéficos para a sociedade: algumas empresas podem alegar que os regulamentos internacionais limitam a livre-iniciativa e o desenvolvimento de tecnologias que visam o progresso e o conforto humanos. Além disso, existe um acordo entre a empresa e o usuário sobre a privacidade e uso dos dados, estabelecido de maneira livre e consentida. É possível imaginar que as organizações de governo discordem da abrangência daqueles limites impostos, uma vez que a segurança coletiva é um dos deveres do Estado, ainda mais quando as principais ameaças à sua autonomia se organizam na própria rede cibernética.

Quadro 1: Comparação entre as teorias sobre a vigilância na internet

Teoria Panóptica	**Teoria não-Panóptica**
Utiliza a imagem do panóptico para compreender a vigilância na internet nos dias de hoje.	Não utiliza a imagem do panóptico para compreender a vigilância na internet nos dias de hoje.
A vigilância online deve ser entendida como algo negativo para os vigiados.	A vigilância online deve ser entendida de modo neutro, com aspectos negativos e positivos para os vigiados.
Essa posição utiliza uma noção restrita de vigilância.	Essa posição utiliza uma noção ampla de vigilância.
A vigilância na internet está relacionada à coerção, repressão, disciplina, poder e dominação.	Existem efeitos positivos e negativos na coleta de dados, que nem sempre restringem a liberdade.
O poder é centralizado e a sociedade tende a ser reprimida e controlada.	Antes de ser uma relação de poder, a internet tem aspectos técnicos e tecnológicos distribuídos.

Fonte: Adaptado de ALLMER, 2012, p. 73-74.

Estes dois modos de compreender a vigilância na internet podem servir de fundamento para os posicionamentos éticos e políticos das representações e dos países-membros da ONU durante a simulação da AGNU, no que se refere ao uso de dados pessoais consentidos e não consentidos, ao uso informações sem dono e anônimas, aos novos modos de vida e de sociabilidade em que o monitoramento também ocorre entre indivíduos (que possuem câmeras à mão), ao uso de informações pelo governo e por plataformas políticas etc.

1.1 Governabilidade Algorítmica

O conceito de governabilidade algorítmica refere-se a uma combinação entre a lógica de coerção política dos governos e o uso de dispositivos ultratecnológicos de controle dos indivíduos, neste caso, o investimento em desenvolvimento de algoritmos. Do ponto de vista técnico (teoria não-Panóptica), o que é um algoritmo? É uma sequência lógica de ações necessárias para se chegar a um resultado ou produto final. Façamos uma analogia: ao cozinhar é preciso seguir o passo a passo da receita

para se chegar ao prato pretendido. Não é possível levar uma massa ao forno sem antes misturar os ingredientes na ordem determinada pela receita. De forma semelhante, um algoritmo possui uma estrutura que organiza as instruções para que um dispositivo receba uma entrada de dados (os ingredientes), os processe (o modo como eles se organizam) e em seguida apresente uma saída (a refeição pronta). Assim como existem várias receitas diferentes para um mesmo prato, existem tipos de algoritmos com nível de eficiência e instruções diferentes para resolver um único problema ou executar processos iguais. Medina e Fertig (2006) definem o termo algoritmo como um procedimento metódico para a solução de um problema, isto é, uma sequência detalhada de ações a serem executadas automaticamente para realizar alguma tarefa. Portanto, para que um computador funcione é necessário que alguém programe essa sequência de maneira lógica e bem estruturada, e informe ao computador, para que este possa executar os comandos. Uma imagem simples do funcionamento dos algoritmos em nossas vidas é a seguinte:

> Imagine-se combinando com amigos, via celular, uma saída noturna. Vocês pensam em cinema, talvez uma janta (...). Enfim, qualquer diversão que promova o encontro e a boa conversa. Após a pesquisa no buscador preferido e feita a escolha entre as opções oferecidas, vocês inserem o nome do estabelecimento no aplicativo de localização e, em seguida, chamam o serviço de transporte. O valor da corrida será debitado no cartão de crédito. Nestes minutos de utilização de aplicativos e outros serviços via Internet, com alguma passagem nas redes sociais, enormes bases de dados receberam e transmitiram informações em torno de suas movimentações. Perante este acúmulo de entradas e saídas de dados, o indivíduo realiza seus desejos sob o custo de tornar-se mera engrenagem. As máquinas, cujas nuvens de informações pairam através, sobre e entre nossas vidas, mitigam as distâncias entre os mundos físico e virtual, acionando e satisfazendo necessidades coletivas e singulares (TELES, 2018, p. 430).

Podemos entender como computador qualquer máquina programável capaz de receber, processar e retornar informações, por exemplo, uma calculadora que recebe os números e a operação a ser realizada é capaz de retornar um resultado. Quando falamos em algoritmo, estamos nos referindo justamente a esse processamento de dados. Uma máquina não é capaz de pensar por si, isto é, ela precisa estar previamente programada para funcionar. Os algoritmos servem para programá-la. Muitas vezes, essa programação faz elas sejam capazes de se autoajustar diante do imprevisto, reparar algum mau funcionamento e adaptar-se ao ambiente. Segundo Manzano e Oliveira (2016, p. 21),

> o processo de programação é uma "conversa" controlada entre um ser humano (tecnicamente preparado) e o computador propriamente dito. O processo de comunicação se faz com o uso de uma linguagem de programação que o computador "entenda".

Uma vez escrito em linguagem de programação – bastante semelhante à sintaxe das

linguagens humanas –, o algoritmo deve ser compilado, isto é, convertido para a linguagem de máquina. Desta forma, os comandos e as instruções serão transmitidos e executados pelo computador. As vantagens desta tecnologia são: a comodidade, a rapidez dos serviços, a economia de tempo e dinheiro, a eficiência nos resultados das buscas, entre outras. É como se o computador, depois de programado com o algoritmo correto, soubesse mais de nossas vontades e pensamentos do que nós mesmos, e pudesse calcular uma rota de ação mais benéfica do que jamais poderíamos imaginar.

Do ponto de vista da teoria Panóptica, significa também que estamos presos a esse ciclo de programação: os nossos dados são recolhidos, processados, analisados e retornados em forma de estímulo para determinado comportamento, que se transforma em dado recolhido, processado e assim por diante. Para os indivíduos e para os que governam, a questão central é: qual o custo deste ordenamento social? A resposta, para os indivíduos, gira em torno da perda da liberdade e da anulação de suas subjetividades. Para o governo, a resposta é resultado de um cálculo algorítmico que antecipa os comportamentos possíveis e permite escolher, entre estes, qual se transformará em norma e lei.

1.2 *Big data*, Mineração de dados e *Socialbots*

Os avanços tecnológicos da sociedade em rede possibilitam a **hipercomunicação**, isto é, a troca e o exame massivos e ininterruptos das informações. As mais diversas ações diárias da população mundial (uso de redes sociais, registros corporativos, transações financeiras, conversações etc.) geram dados valiosos que podem ser utilizados, por empresas e por governos, para entender o comportamento de um grupo de pessoas e para conseguir melhorar suas campanhas de marketing. Em um mundo cada vez mais competitivo, a utilização de técnicas e ferramentas para se manter à frente nos negócios tem se tornado indispensável. De modo simplificado, os Big Data se referem à análise computacional de grandes conjuntos de dados, cujo objetivo é revelar padrões e tendências. Os Big Data representam, portanto, o grande volume de dados transmitidos pela internet em alta velocidade e com grande variedade.

As técnicas de Mineração de Dados podem ser divididas em quatro tipos: classificação, regressão, predição e associação. A classificação consiste em determinar a qual classe um determinado dado pertence. Já a regressão tenta estimar o valor numérico de uma variável, como a nota de um aluno em uma determinada matéria com base em suas outras notas. A predição tenta descobrir o valor futuro de uma determinada variável, por exemplo, qual o valor de uma ação no futuro. E por último a associação que consiste em identificar relações entre os dados. As regras de associação são conhecidas como "cesta de compras", pois são comumente utilizadas para identificar os produtos que são mais comprados em conjunto.

A cada ano aumenta a quantidade de dados transmitidos e armazenados. Estima-se que a quantidade de dados no mundo crescerá de 4,4 trilhões de gigabytes em 2013 para 44 trilhões de gigabytes em 2020 (EMC, 2014; Graf. 1). O conjunto de dados será tão grande que não poderá ser analisado por *softwares* convencionais de computadores normais. As ferramentas e algoritmos capazes de processá-los e

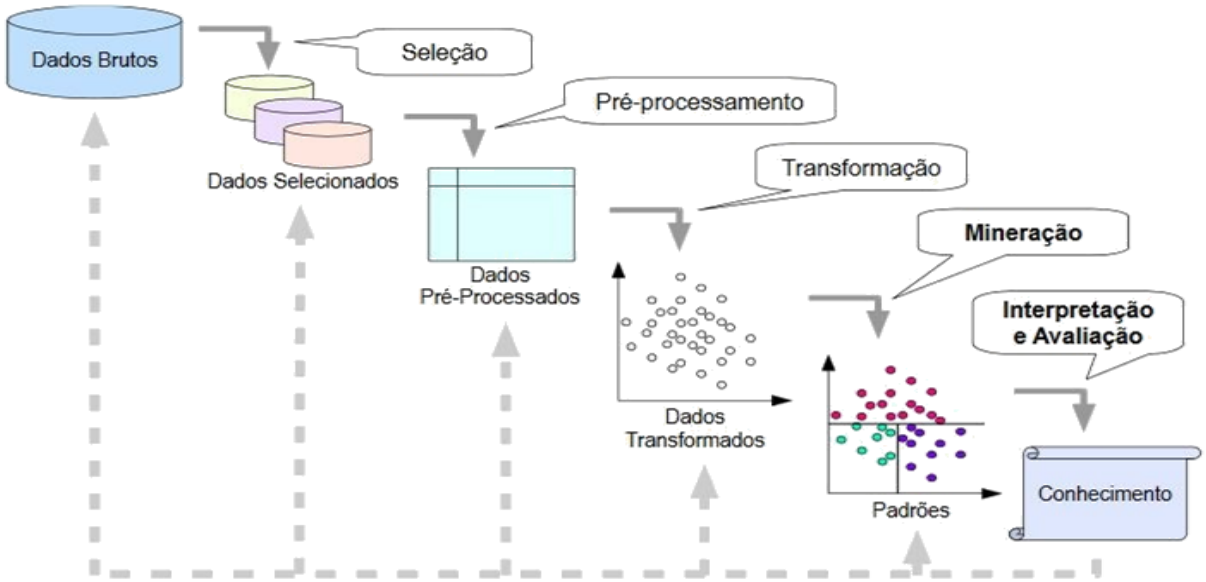
gerar informações importantes economicamente exigirão investimentos massivos em *hardwares* de armazenamento e processamento.

O uso de técnicas algorítmicas para buscar informações relevantes dentro dos imensos repositórios de dados pode oferecer ajuda nas tomadas de decisão governamental. Dentre essas técnicas está a **Mineração de Dados**, isto é, uma etapa do processo denominado Descoberta de Conhecimento em Banco de Dados (DCBD). Esta é uma metodologia para descobrir as informações mais relevantes dentro do repositório (Fig. 2), constituído por dados brutos recolhidos em "redes sociais, blogs, *feeds* de notícias, dados de sensores de faces, sons e imagens, e-mails, jogos, geolocalizadores e autorizações de celulares, sistemas de cartões, operações de marketing e publicidade, pesquisas científicas, redes e sistemas de segurança" (TELES, 2018, p. 435).

A mineração de dados é, portanto, uma técnica que procura extrair conhecimento (Fig. 2). Entretanto, a extração ainda não ocorre de maneira automática (*machine-learning*), conforme observa Camilo e Silva (2009), já que o significado do resultado do processo, a interpretação, a avaliação e a valoração também são atividades humanas.

Devido à variedade de sujeitos e comportamentos possíveis, os Big Data ganham valor após a mineração, quando é possível encontrar um padrão, isto é, a predição do modo mais adequado de se estabelecer um comportamento. O perfil dos usuários é classificado de acordo com a predição obtida pelas técnicas de perfilhamento automatizado (*profling*). Assim, todo discurso e toda informação heterogênea aos interesses dos indivíduos são descartados após o cálculo dos algoritmos, de modo a mantê-los em suas próprias *bolhas* ideológicas e indentitárias, cada vez mais fechadas a discordâncias, debates e respeito a diferenças, características fundamentais, de acordo com a ONU, para o estabelecimento de uma sociabilidade plena e democrática.

Figura 1: Processo de mineração de dados



Fonte: Santos (2009).

Recentemente, a ONU constituiu Comissões Eleitorais Independentes com o objetivo de acompanhar e aferir a correção de processos eleitorais de vários países. A ONU enviou missões a Gana, Mali, Bangladesh, Guiné-Bissau, Costa do Marfim, Congo, China, Venezuela etc. O objetivo é garantir a normalidade institucional deste importante ritual democrático.

Um tópico relevante para a Assembleia Geral das Nações Unidas é o uso de tecnologias que interferem na legitimidade dos debates políticos na internet. Estamos falando da utilização em massa de perfis falsos automatizados que interagem no ciberespaço: os chamados *socialbots* (robôs sociais). Eles imitam o comportamento humano e corrompem o debate público de modo a criar

> a falsa sensação de amplo apoio político a certa proposta, ideia ou figura pública, modificam o rumo de políticas públicas, interferem no mercado de ações, disseminam rumores, notícias falsas e teorias conspiratórias, geram desinformação e poluição de conteúdo, além de atrair usuários para links maliciosos que roubam dados pessoais, entre outros riscos (RUEDIGER, 2017, p. 9)

A ação dos *socialbots* pode ter interferido em debates e no processo eleitoral de importantes democracias como a da França, Alemanha, Reino Unido (*Brexit*), Estados Unidos (eleições de 2010 e 2016), Paraguai e Brasil (reforma trabalhista). A detecção e a eliminação dos *socialbots* são desafios globais e cada vez mais complexos, já que os robôs virtuais aprendem a emular o comportamento humano por meio da técnica de *machine-learning*. Os compartilhamentos coordenados e volumosos de determinadas versões ou falsificações de fatos, por meio de links espalhados nas redes sociais, revelam os riscos da desinformação e da perda da capacidade crítica de sabermos diferenciar o verdadeiro e o falso. Os direitos à opinião e à expressão de informações são preceitos da DUDH (art. 19), desde que estas manifestações ocorram "sem interferência". O quanto de interferência há no ciberespaço? Como podemos diminuir as interferências e assegurar a liberdade de expressão plena? No fundo, o esforço da ONU é no sentido de assegurar que as leis e práticas domésticas relacionadas à internet acompanhem os padrões internacionais dos direitos humanos.

Os *socialbots* podem se classificar em três grupos: Duplicadores (que multiplicam a mesma mensagem a partir de outros perfis), Promotores maliciosos (que postam serviços comerciais ou inflam artificialmente as *hashtags*), e Infiltradores de amizade (que se baseiam em reciprocidade, e pretendem ser influenciadores).

1.3 Segurança na rede: Deep Web, Hackers e Crackers

As redes de computadores se tornaram indispensáveis para o compartilhamento de recursos e, principalmente, de informações. Independentemente da localização de um indivíduo, desde que exista acesso à internet, é possível estabelecer uma comunicação com outros usuários e utilizar serviços disponíveis nos servidores espalhados pelo mundo. Quando nos referimos ao termo **servidores** estamos

falando de máquinas que disponibilizam serviços (por exemplo, o e-mail) e permitem o compartilhamento entre os **usuários**, que são consumidores ou clientes desses serviços. Estabeleceram-se regras para a comunicação na internet, chamadas de protocolos, que definem padrões para que as máquinas troquem dados entre si, como um idioma único utilizado e entendido por computadores do mundo inteiro.

A criptografia é uma técnica de combinar e analisar protocolos em um ambiente de comunicação, de modo a assegurar que um agente externo não tenha acesso aos dados do emissor e do receptor das mensagens. As *chaves* da criptografia e descriptografia são geradas por algoritmos. Quando inserimos nossas senhas em sites confiáveis, essas informações são criptografadas através de um protocolo de segurança.

Um dos principais protocolos é o *Internet Protocol* (IP). Segundo Tanenbaum (2003), o IP foi estruturado para permitir a interligação das redes e tem como objetivo transportar o fluxo de dados (divididos em pacotes) do remetente até seu destinatário, seja em uma rede local (*intranet*), restrita a clientes (extranet) ou nacional (para os Estados-nação). Sendo assim, o IP pode ser entendido como um conjunto de números atribuídos a todos os dispositivos conectados à rede, identificando o usuário e a sua localização. De forma análoga, podemos enxergar esse sistema como o transporte de encomendas via Correios: para que elas sejam enviadas o remetente deve especificar o endereço de seu destinatário (cidade, bairro, rua, cep etc.), o que permitem localizar exatamente onde, por quem e para quem devem ser entregues.

Porém, a facilidade e a liberdade disponíveis nessa forma de compartilhamento de informações geram riscos de invasão e violação – como se alguém, além do próprio entregador dos Correios pudesse violar, rastrear ou bisbilhotar a encomenda enviada. Por isso, como medida protetiva contra essas ameaças existe o **firewall**, um mecanismo que monitora e filtra o tráfego de informações transmitidas pela rede de acordo as políticas de segurança estabelecidas. Redes Nacionais, por exemplo, podem alegar questões de segurança e limitar o acesso de seus habitantes a sites específicos. Tanenbaum (2003) compara o firewall com uma medida de segurança medieval: para proteger-se era necessário cavar um fosso em torno do castelo. Assim, qualquer um que tentasse entrar ou sair daquela área deveria passar por uma ponte levadiça e ser revistado por guardas. O firewall seria essa ponte por onde o fluxo de dados trafega e é submetido à verificação pelo sistema de segurança. Hoje, esse mecanismo já vem incluso em dispositivos como computadores, roteadores e modens. Mesmo assim, ele não oferece segurança total e pode ser alvo de ataques externos. Logo, as redes necessitam de sistemas de proteção adicionais e políticas de segurança que definam normas para que as informações compartilhadas não percam atributos considerados indispensáveis, tais como a confidencialidade, integridade e a disponibilidade. As informações devem provir de fontes confiáveis. Elas devem estar completas e não fragmentadas. Por fim, as informações devem estar disponíveis ao acesso.

Por onde se navega na internet, no ciberespaço, encontram-se tanto conteúdos bons para estudos e lazer, quanto conteúdos e caminhos perigosos e danosos, em relação aos quais não é possível estabelecer os três atributos citados. Um destes locais é a chamada **Deep Web**. Segundo Franco e

Magalhães (2015), a Deep Web (*dark web*, *deepnet*, *invisible net*, *undernet*, ou *hidden web*) refere-se a toda rede fechada que compreende um grupo privado de pessoas, que querem se comunicar sem as restrições de seguridade. Trata-se da camada da internet que não pode ser acessada por um navegador comum (que exige os protocolos de segurança). Podemos fazer uma analogia com um iceberg: a internet normal (a ponta que está a mostra) corresponde a uma pequena parcela do universo e a Deep Web corresponde a todo o resto que está submerso e imperceptível ao usuário comum. Nela se encontram diversas organizações criminosas, bem como fóruns que ensinam a construir bombas, grupos que espalham preconceito e xenofobismo, vendem drogas proibidas em grande parte dos países, estimulam e comercializam órgãos humanos e pessoas, e mais além. No geral esses tipos de compartilhamento ocorrem de forma anônima. A principal diferença em termos técnicos é que na Web do usuário comum, tudo que acessamos ou fazemos pode ser rastreado, pois as páginas são geralmente indexadas. Na Deep Web pouca coisa pode ser rastreada. Aqui as páginas não são indexadas e possuem muitos **dados criptografados**, reforçando o anonimato e impedindo o rastreamento da origem das informações.

Ao falarem de Segurança da Informação, Barbosa e Silva (2016) definem alguns tipos de ataques: os ataques diretos envolvem o contato pessoal; os indiretos utilizam ferramentas para obtenção de dados, como e-mails falsos, sites maliciosos e cavalo de Tróia. Dentro desse universo surge o Hacker, isto é, "um indivíduo que objetiva explorar minuciosamente os sistemas e descobrir como obter o máximo de sua capacidade" (COSTA et al., 2012, p. 84). Por definição, o *hacker* nem sempre age de maneira utilitarista e maliciosa. São os chamados *crackers* quem colocam a nossa segurança e privacidade em risco. Segundo Basta et al. (2014), o termo *cracker* se refere a quem está do "lado obscuro" da computação, são hackers que se dedicam a destruir e roubar informações. Eles são os verdadeiros criminosos virtuais, pois quebram a segurança de sistemas com objetivos financeiros ou políticos. Grupos de hackers ativistas políticos, como o Anonymous e o Shadow Brothers, cometem o ciberterrorismo com o objetivo de subverter a lógica de vigilância na internet.

Existem ameaças que visam escapar da autenticação e da criptografia normalmente exigidos pelo sistema computacional, como o *ransomware*, que sequestram dados com vistas a um resgate financeiro, e o *backdoor*, que vaza as informações sem alertar os dispositivos de segurança. Empresas e governos investem massivamente na segurança dos hardwares (limitação física de acesso), na proteção de dados e arquivos (autenticação, controle de acesso virtual e antivírus) e na proteção do perímetro da rede (criptografia, firewalls). Com o propósito de melhorar a segurança de sistemas, existem normas e testes de segurança, como o Teste de Penetração (*Pentest*), que funciona simulando a tentativa de penetrar um sistema com objetivo de descobrir "falhas, aberturas, rastreando por completo todo o sistema, realizando uma auditoria completa" (MENESES et al., 2015, p. 88). É comum grandes corporações contratarem este tipo de serviço, tanto para descobrirem brechas na sua política de segurança, quanto para explorar dados e informações no ciberespaço que lhes deem alguma vantagem competitiva.

1.4 Privacidade individual versus segurança coletiva na internet

O que pode justificar a aceitação da perda de privacidade? As ameaças de terrorismo são suficientes para abandonarmos este direito? De fato, a privacidade parece estar mais próxima do direito à liberdade (isto é, de possuir uma subjetividade e desenvolvê-la de maneira autônoma) do que do direito à segurança. Podemos explorar uma lista de ameaças ou "males" da internet que justificam a precaução diante do **ciberterrorismo**: termos em inglês como *worms*, *malware*, *spyware*, *socialbots*, *trojan, back door, crackers* e *phishing, deep web* compõem a taxonomia das ameaças virtuais a que estamos sujeitos no ciberespaço. A grande questão deste debate é a seguinte: a privacidade nas redes também é uma ameaça à segurança?

Por um lado, pode-se pensar que o direito à privacidade plena seja um atalho para os crimes cibernéticos e sirva de proteção para os criminosos estimularem a pornografia infantil, a pedofilia, o racismo e a homofobia, advogarem o neonazismo e a intolerância religiosa, incitarem maus-tratos contra os animais e crimes contra a vida, intimidarem pessoas e as subornarem, *hackearem* contas bancárias, e-mails, documentos e fotos pessoais, praticarem a pirataria e a violação dos direitos autorais, distribuindo conteúdos protegidos etc.

Por outro lado, deve-se levar em conta a diferença entre o anonimato e a neutralidade nas redes. Em geral, considera-se que a liberdade de expressão não é compatível com o anonimato, pois este inviabiliza o direito de resposta (no caso de uma ofensa ou um debate justo) e restringe o direito de acesso completo à informação. Ainda assim, a ONU recomenda que os países-membro sejam cautelosos ao regulamentarem penalmente o anonimato: ideias ambíguas e vagas como "combate ao ódio", "extremismo", "blasfêmia", "linguagem ofensiva", "notícias falsas" etc., não podem servir de subsídio jurídico para que os países construam leis restringindo as liberdades nas redes e fora delas. No *Relatório Especial sobre as Tendências Mundiais sobre Liberdade de Expressão e Desenvolvimento da Mídia*, a UNESCO defende o pluralismo de ideias e condena a censura prévia como maneiras de combater o próprio crime cibernético, tendo a imprensa papel fundamental na divulgação das irregularidades, como no caso da NSA (ver Seção 1.5).

O **princípio da inimputabilidade** diz respeito à garantia de que os provedores, os aplicativos de acesso à internet e os seus conteúdos não sofrerão censura, exceto em casos excepcionais e após o julgamento dos recursos em âmbito jurídico. Neste caso, as empresas de intermediação não podem ser culpadas nem terem seus serviços bloqueados por causa de um conteúdo qualquer. Isso estimula a criatividade e a livre iniciativa, já que novos protocolos experimentais são aceitos e geram conteúdos criativos, como *memes*, *mashups* e bricolagens, isto é, criações e manifestações culturais ou

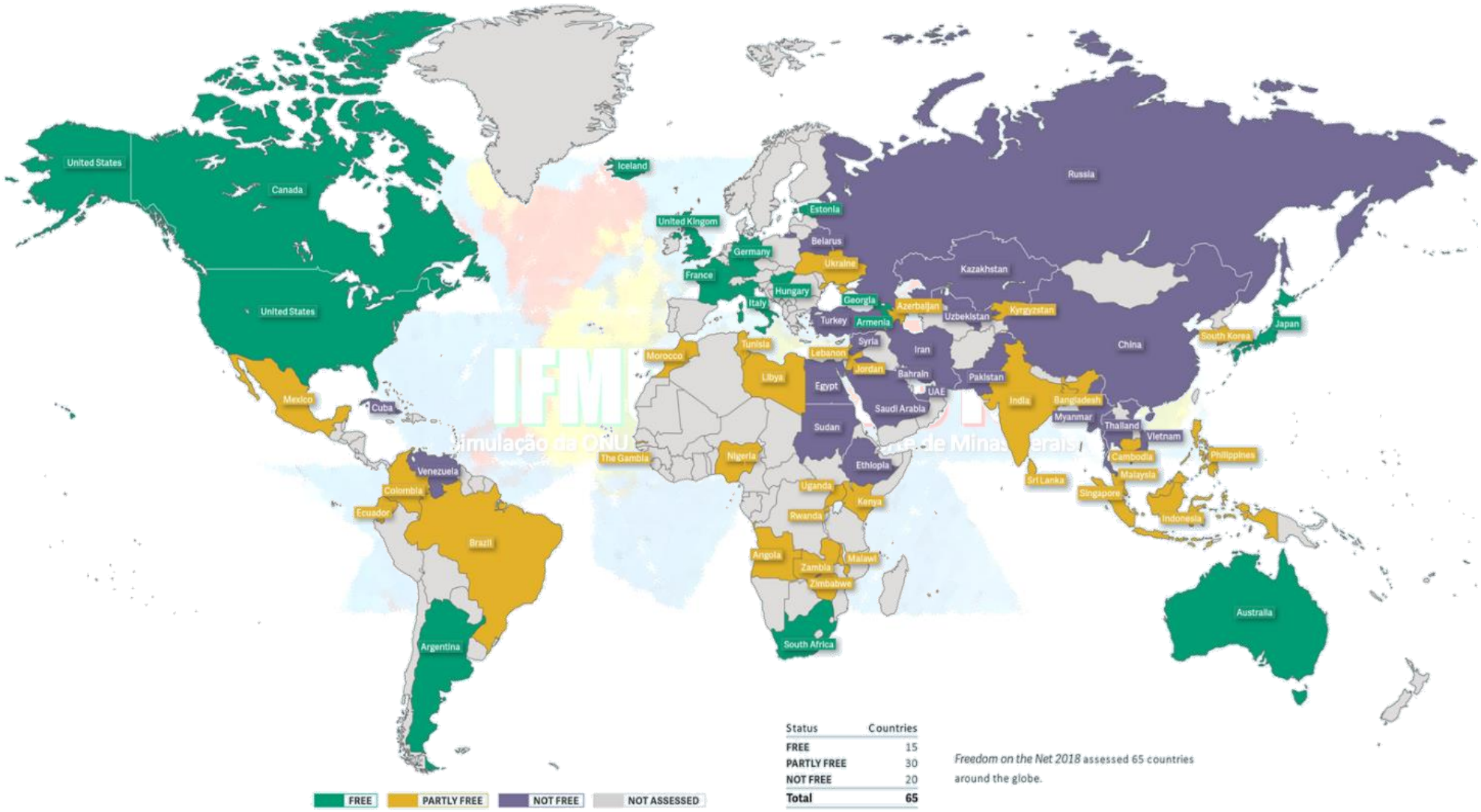
políticas que não deveriam ser restritas pela alegação, por exemplo, de violação de direitos autorais.

O **princípio de neutralidade** diz respeito à garantia de que as operadoras de banda larga ou responsáveis pela infraestrutura dos cabos não interfiram ou priorizem os conteúdos a serem acessados pelos usuário e clientes. De acordo com o princípio, as empresas podem até cobrar por pacotes de internet com maior velocidade, mas não podem limitar os conteúdos (por exemplo, cobrar a mais para o usuário acessar determinado site) nem vender pacotes fechados (por exemplo, limitar as transferências de *dowloads* a 10gb). As empresas e os governos, portanto, deveriam ser neutros tanto em relação aos pacotes de dados que trafegam pela sua infraestrutura, quanto em relação aos conteúdos acessados pelos usuários, não podendo filtrar, monitorar, analisar o seu conteúdo, tampouco restringir os seus direitos fundamentais. Na prática, a neutralidade significa que um vídeo do Youtube tem a mesma prioridade de transferência do que uma mensagem no Whatsapp. A Figura 2 e o Gráfico 2 mostram o mapa global da neutralidade na rede. Governos e empresas de tecnologia podem se beneficiar da neutralidade, uma vez que a interrupção de serviços na rede custa bilhões de dólares ao ano, impactando na produtividade e na confiança de consumidores e investidores.

Para compreender o alcance político e antidemocrático das "bolhas ideológicas", que resultam de cálculos algorítmicos, Eli Parise (2012) propõe que se faça um teste simples: peça a pessoas de diferentes ideologias políticas para pesquisarem no buscador do Google sobre um acontecimento marcante do dia. Em seguida, compare o conteúdo das notícias. Você perceberá que o buscador varre as notícias que, segundo os algoritmos, não estão de acordo com os perfis, isto é, de acordo com o que a máquina "pensa" que gostaríamos de conhecer (mesmo que seja a informação falsa) e não com o que necessitamos conhecer (mesmo que seja a informação verdadeira)

O Conselho de Direitos Humanos da ONU, em 2016, que o acesso à internet é um direito humano, reconhecendo que a sua natureza aberta pode acelerar o progresso social e atingir os objetivos do desenvolvimento sustentável (OHCHR, 2016). Além disso, a ONU criou o Fórum de Governança na Internet (*Internet Governance Forum* – IGF) para debater o modelo de organização das redes. O ciberespaço tornou-se uma **plataforma política internacional**, onde as vozes e subjetividades podem se expressar e criar um ambiente democrático, mesmo que, do ponto de vista da estrutura global de telecomunicações, parte significativa dos fluxos de dados ainda passe pelos Estados Unidos (BEZERRA, 2014, p. 160). A dispersão do controle de Washington para organismos multilaterais como a própria ONU poderá fazer com que seja necessário discutir um novo pacto global de governança na internet (**RGDP.ONU)**, pautado pelos seguintes princípios: **privacidade**, a **neutralidade** e a **inimputabilidade da rede**.

Figura 2: Mapa global da neutralidade nas redes

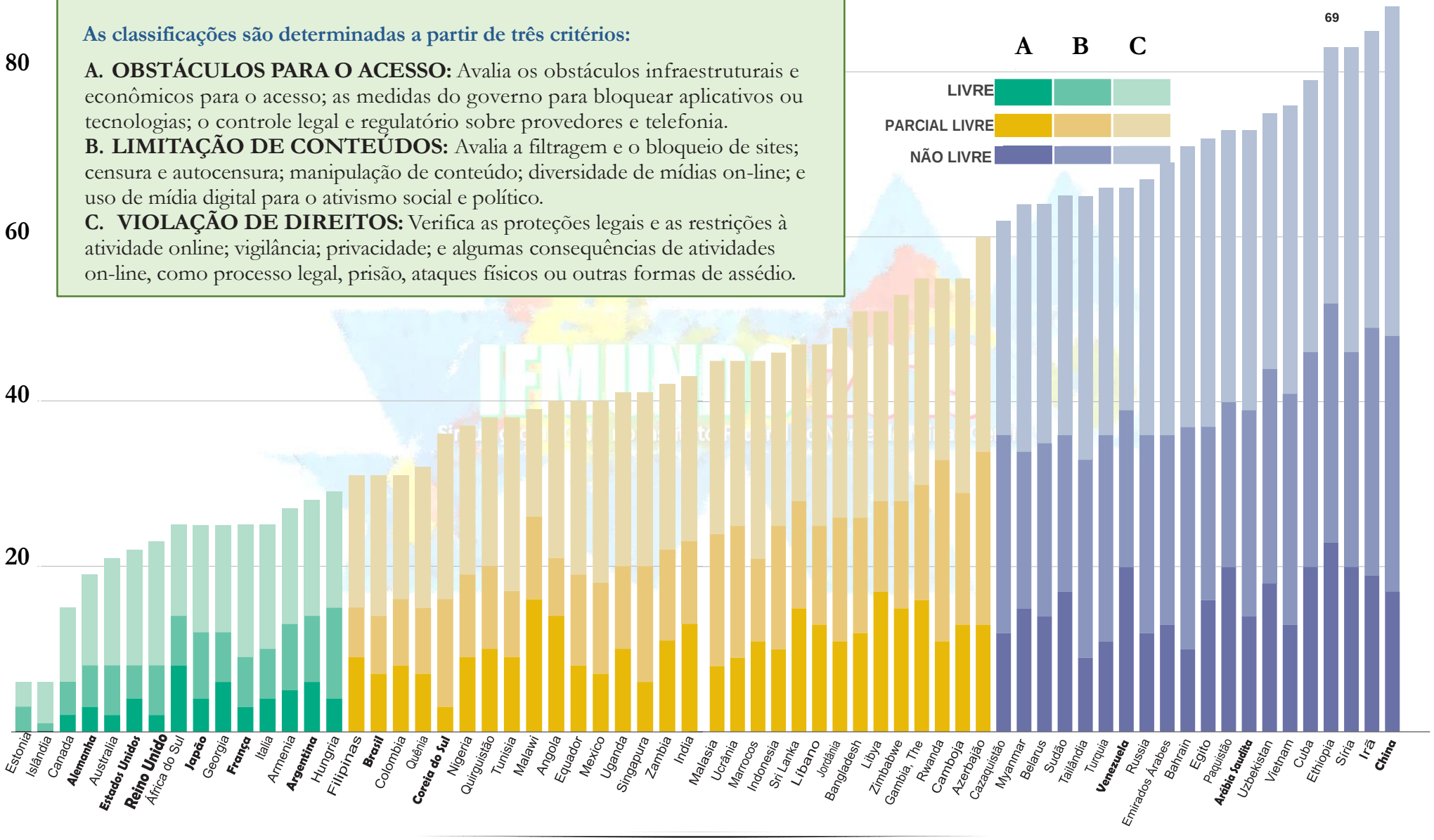


Fonte: FOTN, 2018, p. 16-17.

Gráfico 2: Nível de liberdade da internet. Cada país recebe uma pontuação de 0 a 100: LIVRE (0-30), PARCIALMENTE LIVRE (31-60), ou NÃO LIVRE (61-100). FONTE: FOTN, 2018, p. 24-25.

As classificações são determinadas a partir de três critérios:

A. OBSTÁCULOS PARA O ACESSO: Avalia os obstáculos infraestruturais e econômicos para o acesso; as medidas do governo para bloquear aplicativos ou tecnologias; o controle legal e regulatório sobre provedores e telefonia.
B. LIMITAÇÃO DE CONTEÚDOS: Avalia a filtragem e o bloqueio de sites; censura e autocensura; manipulação de conteúdo; diversidade de mídias on-line; e uso de mídia digital para o ativismo social e político.
C. VIOLAÇÃO DE DIREITOS: Verifica as proteções legais e as restrições à atividade online; vigilância; privacidade; e algumas consequências de atividades on-line, como processo legal, prisão, ataques físicos ou outras formas de assédio.



1.5 O caso da NSA

Fonte: https://www.snowdenfilm.com/

No filme SNOWDEN, o protagonista é retratado como um hacker americano patriota diante de um conflito ético: construir ferramentas digitais de vigilância para garantir a supremacia econômica e bélica de seu país ou denunciar o sistema de coleta e uso de dados da população, inclusive a de seu país, pelo governo?

O ex-presidente dos Estados Unidos da América, Barack Obama, uma vez afirmou que "não se pode ter 100% de segurança e também ter 100% de privacidade sem ter nenhum inconveniente" (GUARDIAN, 2015). A frase foi dita em 2013, após Edward Snowden revelar o alcance das práticas de vigilância do governo dos Estados Unidos.

Snowden foi um funcionário das agências norte-americana de inteligência, defesa e segurança (CIA, DIA e NSA), recrutado pelo departamento de proteção às redes de comunicação, interceptação e criptografia de dados digitais.

Segundo as denúncias de Edward Snowden, além dos dados telefônicos, o software de vigilância Prism, usado pela NSA, coletava dados de provedores online incluindo e-mail, serviços de chat, vídeos, fotos, dados armazenados, transferências de arquivos e senhas. Entre as empresas envolvidas estavam grandes empresas de tecnologia como Microsoft, Facebook, Google (incluindo o YouTube) e Skype (GREENWALD, 2014).

De acordo com as denúncias de Snowden, o governo americano tirou vantagem do fato de ter desenvolvido, durante a corrida de armamentos da guerra fria, grande parte da infraestrutura da internet (arquitetura de cabos submarinos, servidores, sistema de identificadores e protocolos, indústrias e polos tecnológicos, fabricantes de softwares, produtores de hardwares). O barateamento da tecnologia de computação permitiu que, em vez das antigas formas de vigilância direcionada, a coleta de informações pudesse ser feita em massa, no século XXI. Isso significa que é possível armazenar e analisar todas as telecomunicações, todas as chamadas de voz, todo o tráfego de dados e todas as mensagens de texto (BEZERRA, 2016, p. 231).

De acordo com a denúncia, o Departamento de Defesa dos Estados Unidos pretendia manter o controle militar do ciberespaço, com a justificativa de proteger-se de atentados terroristas como o de 11 de setembro de 2001. Para os jornalistas que acompanharam Snowden, as práticas de vigilância escondiam as intenções do controle geopolítico e da expansão econômica, já que o governo norte-americano teria informações privilegiadas e antecipadas sobre qualquer outro ator político e econômico do mundo. Snowden revelou a jornalistas que a NSA obteve dados de empresas petrolíferas no Brasil (Petrobrás) e na Venezuela (PDVSA), espionou "ocasionalmente" o Fundo Monetário Internacional e o Banco Mundial, mapeou a movimentação das Forças Revolucionárias da Colômbia, fiscalizou a empresa de energia no México e outras entidades na América Latina, espionou países suspeitos de abrigarem

terroristas como o Irã e o Paquistão, monitorou as comunicações de países como a China, "grampeou" (telefone, chamadas de voz e e-mail) diversos líderes políticos, entre presidentes, chanceleres e ministros de estado, além de espionar organizações como a Anistia Internacional.

Atualmente, Snowden encontra-se asilado na Rússia, mas participará da simulação da Assembleia Geral das Nações Unidas protegido por um *Habeas Corpus* impetrado junto à Corte Internacional de Justiça.

No ordenamento jurídico internacional, os documentos de trabalho podem ser de vários tipos, sendo os principais:

1) **Regulamento**: conjunto de normas vinculativas que devem ser seguidas pelos países signatários. Regulamentos internacionais têm o mesmo poder das leis nacionais.
2) **Diretiva:** objetivos a serem alcançados por um conjunto de países, cabendo a cada um estabelecer a forma de se alcançar os objetivos.
3) **Recomendação:** parecer não vinculativo, com a função de orientar a tomada de decisão dos países ou declarar a posição do organismo comunitário sobre uma questão.
4) **Decisão**: em formato de resolução ou declaração, a depender do estatuto da organização, obriga apenas os Estados-membro que a

2 Posição dos principais atores

Um relato individualizado de cada país em relação à liberdade na internet pode ser encontrado (em inglês) aqui: https://freedomhouse.org/report/countries-net-freedom-2018.

As informações abaixo dizem respeito aos regulamentos e leis domésticas sobre a internet. Estes regulamentos expressam o modo como as delegações podem se posicionar sobre o Regulamento Geral de Proteção dos Dados Pessoais que a ONU pretende estabelecer (**RGDP.ONU**).

2.1 União Europeia (UE)

A União Europeia adotou o Regulamento Geral de Proteção dos Dados Pessoais da União Europeia (RGDP.UE) a partir de maio de 2018. Todos os 28 estados-membros da UE estão diretamente submetidos ao regulamento. O artigo 4º do RGDP.UE define conceitos-chave como "dado pessoal" e "consentimento", além de estabelecer os responsáveis pela proteção dos dados e pela fiscalização do serviço. Qualquer informação que possa indicar uma pessoa é considerada dado pessoal (IP, localização, nome, imagem, endereço etc). São proibidas as coletas sem consentimento de dados sensíveis dos usuários, isto é, aqueles dados relacionados a opiniões políticas, dados genéticos, raciais, orientações sexuais (art. 9º), exceto para fins de medicina preventiva. O pedido de consentimento ao usuário para a coleta e o processamento de seus dados pessoais deve ser redigido de maneira clara e completa, podendo as empresas e os governos serem responsabilizadas (multas e penalidades) pelo uso indevido de dados ou pelo vazamento de informações. Dois novos procedimentos são previstos no RGDP.UE: o "direito ao esquecimento" (art. 17), que permite ao usuário solicitar que os seus dados sejam apagados; o "direito à explicação ou oposição à tomada de decisões automatizadas" (art. 22), que permite ao usuário contestar

a avaliação realizada pelos algoritmos após a mineração de seus dados (POLIDO et al., 2018, p. 11-12). Isso abre a oportunidade para que as empresas de tecnologia construírem algoritmos que não apenas retornem previsões de padrões de comportamento, mas que tenham um senso ético de responsabilidade, de modo a tornar transparente ao usuário as informações filtradas e devolver a ele o controle de suas decisões.

Além de servir como modelo para outras iniciativas nacionais e intracomunitárias, o RGDP.UE aplica-se a atividades fora dos limites territoriais da Europa, por exemplo, quando a operação e o tratamento dos dados de cidadãos europeus forem realizados por empresas de outros países. O modelo europeu apresenta os seguintes pontos em comum com os regulamentos americanos: consentimento, a transparência, os direitos de acesso, retificação e eliminação de dados, e as obrigações de segurança e sigilo. Países membros da UE como a Estônia, Alemanha, França, Itália e Hungria lideram o ranking de liberdade na internet (Graf. 2).

2.2 Estados Unidos

Embora não exista uma lei federal que discipline de maneira abrangente a privacidade na internet, existe um esforço para tratar o tema a partir de setores. Deste modo, criaram-se leis específicas, por exemplo, para regulamentar as transações eletrônicas, para proteger os dados e a privacidade de crianças e adolescentes, e para proteger o sigilo médico (GUIDI, 2017). As agências e organismos de governo estão submetidas ao *Privacy Act* desde 1974, que garante o acesso e a transparência dos atos de governo com interesse público. Da mesma forma, o sistema norte-americano não possui um órgão de controle externo, independente e central para lidar com todas as questões relacionadas ao direito à privacidade. Trata-se de um modelo descentralizado, que se adapta às regras de mercado, na medida em que os usuários e as empresas possuem autonomia para estabelecerem os termos do contrato de privacidade, em geral, instituído na forma de consentimento deliberado, isto é, o usuário tem a possibilidade de ceder voluntariamente os direitos sobre os seus dados pessoais. A Comissão Federal de Comunicação (CFC) é responsável apenas pela supervisão de práticas anticompetitivas entre as empresas. Neste caso, os direitos individuais são garantidos por meio de ações judiciais individuais ou coletivas. Os cidadãos podem alegar o desequilíbrio contratual ou a disparidade de forças entre elas e o provedor do serviço. Desta forma, o governo norte-americano pretende equilibrar dois direitos fundamentais: a privacidade e a livre-iniciativa (GUIDI, 2017, p. 14). No fim de 2017, a CFC revogou os dispositivos de neutralidade na internet, liberando os provedores de acesso da restrição quanto à prioridade de pacotes, conteúdos e velocidades. Além disso, a preocupação com crimes virtuais e com a proliferação de

informações falsas (*fake news*) levou o Congresso a autorizar, por mais seis anos, que o *Foreign Intelligence Surveillance Court* (Tribunal de Vigilância de Inteligência Estrangeira) colete dados e metadados de comunicações dos cidadãos. Os maiores desafios dos EUA são relacionados à disponibilidade e facilitação do acesso à internet (custo da banda larga), à consolidação de um corpo regulatório unificado, ao bloqueio e à remoção de conteúdos (conforme a lei sobre tráfico e exploração sexual), além de cuidar para que escândalos como os da NSA, da Wikileaks e da *Cambridge Analytica* não prejudiquem a imagem nacional da liberdade.

2.3 América Latina

Os modelos de proteção à privacidade na América Latina podem ser vistas como consequências da reafirmação e da expansão dos direitos fundamentais após os regimes ditatoriais, que tinham por prática compilar os dados de seus cidadãos conforme a sua ideologia política (GUIDI, 2017, p. 16).

A lei argentina n. 25.326 (*Ley de Protección de los Datos Personales*) foi promulgada há quase 20 anos. Essa lei colocou a Argentina entre os países com níveis adequados de proteção de dados. A legislação em vigor proíbe a consulta ou a transferência de dados pessoais a países ou entidades estrangeiras que não ofereçam proteção e sigilo. A exemplo da legislação europeia, existe um esforço adicional de instaurar mecanismos de proteção aos cidadãos mesmo nos casos em que o processamento dos dados ocorra a partir da infraestrutura estrangeira. A exemplo da legislação uruguaia, o modelo regulatório argentino instaurou a figura jurídica do *habeas data*, que permite aos usuários recorrerem à justiça em favor de seus dados pessoais, para retificá-los ou exclui-los da rede. Embora a agência de comunicações tenha aprovado a fusão entre duas empresas concorrentes – o que poderá tornar o acesso à internet mais caro –, a Argentina figura entre os países com maior liberdade na intenet, tendo investido maciçamente em infraestrutura de tecnologia.

O Brasil aprovou o Marco Civil da Internet (Lei n. 12.965/2014), sobretudo após ter sido alvo de espionagem da NSA. Esta lei visa a garantir a neutralidade da rede e a privacidade de seus usuários, estabelecendo direitos e deveres, determinando as diretrizes regulatórias do Estado, e impondo responsabilidades aos provedores. O modelo brasileiro está em acordo com o as regras constitucionais de um Estado provedor de serviços e direitos. A internet possui uma função social, promotora dos direitos humanos. De acordo com o Marco Civil, o acesso à internet é "essencial ao direito da cidadania" (art. 7º). A legislação brasileira é bastante nova, se comparada aos países vizinhos. Por isso, ela ainda está sujeita a adaptações, sobretudo no equilíbrio entre os direitos da liberdade de expressão e da segurança

na rede e inviolabilidade dos dados. O ambiente de liberdade on-line brasileiro ainda encontra desafios: várias ordens judiciais de bloqueio do WhatsApp, seguidas de perseguição anônima a blogueiros e jornalistas independentes, bem como a preocupação com conteúdos falsos disseminados durante e após a eleição de 2018.

2.4 China

A China, classificada em última colocada no Índice Internacional de Privacidade, é o país com a lei de segurança cibernética mais restritiva do mundo. Entre outras coisas, permite ao governo censurar informações e sites, restringe as regras de armazenamento online de dados e proíbe acesso a conteúdos considerados subversivos. Entre os chineses, estima-se que aproximadamente 730 milhões de habitantes tenham acesso à internet, dos quais 95% tem acesso à internet móvel, o que equivale praticamente a quase toda a população europeia (743 milhões). Em relação ao acesso do governo aos dados, há a previsão de que, até 2020, o governo chinês instalará um sistema nacional de crédito social que, através da vigilância por vídeo do comportamento público, financeiro e profissional de cada cidadão, atribuirá a eles uma espécie de classificação ou nota. O método de classificação é baseado em um sistema de reconhecimento facial que captura os seus rostos. Os transeuntes identificados por câmeras são informados se estão tendo mau comportamento em tempo real, e podem inclusive receber multas. Além disso, o sistema será capaz de identificar infratores reincidentes e informar a todos que estiverem ao seu redor. Estas medidas de governo visam atender os preceitos constitucionais da República Popular da China, de que o Estado deve ser responsável pela segurança da população, mesmo que, para isso, tenha que restringir alguns outros direitos fundamentais, como a liberdade.

Em junho de 2017, uma nova lei de cibersegurança entrou em vigor no país, aumentando os dispositivos de censura, determinando a localização de dados e obrigando os provedores de internet a auxiliarem as agências de segurança em casos de investigações criminais. As novas regras aumentaram os custos operacionais de administrar uma empresa de internet na China e impediram que a mídia independente tivesse condições de trabalho. Do ponto de vista técnico, o governo central tomou medidas para restringir o uso de ferramentas de anonimato nas redes, consolidando o chamado Grande Firewall Chinês, que filtra notícias e serviços contrários aos interesses do governo. O plano do presidente Xi de transformar a China em uma "superpotência cibernética" inclui medidas de exportação da infraestrutura tecnológica, de modo a dar a oportunidade a países do mundo de conhecer e utilizar do sistema de controle e segurança de informações chinês (FOTN, 2018).

2.5 Rússia

A Rússia é classificada como terceira colocada na parte inferior do Índice Internacional de Privacidade. No país, não há salvaguardas democráticas ou proteções constitucionais voltadas à privacidade. Ao contrário, prevê-se que todos os dados relacionados às telecomunicações ou tráfego na internet devem ser armazenados pela empresa provedora por seis meses, e os dados relacionados a tais comunicações por três anos, à disposição do governo. Além disso, o governo monitora e-mails e redes sociais, e são proibidos aplicativos de troca de mensagens que permitam identidades anônimas, o que viabiliza ao governo rastrear e identificar facilmente qualquer opositor. Quaisquer publicações ou diálogos considerados críticos pelo governo podem resultar em acusações criminais. Nesse sentido, avaliação realizada pela ONG Repórteres sem Fronteiras coloca a Rússia nas últimas posições mundiais em relação à liberdade de imprensa (RSF, 2018).

Com efeito, de 2014 a 2016 85% das condenações penais por manifestações públicas consideradas prejudiciais ao país estavam relacionadas com comunicações na rede. Em 2018, as autoridades russas bloquearam o aplicativo de comunicação Telegram por se recusar a fornecer chaves de criptografia para o Serviço de Segurança Federal, resultando em um amplo bloqueio de garantias e protestos em todo o país. Este bloqueio foi similar ao que aconteceu no Brasil, em 2017, com o WhatsApp. Novas leis estão sendo sancionadas para restringir o anonimato, limitar o uso de redes sociais privadas e garantir a legalidade de sites piratas ou daqueles que distribuam conteúdo que desabone a "honra, a dignidade ou a reputação comercial" (FOTN, 2018).

3 Questões relevantes para o debate

A. Considerando que o acesso à internet é um direito humano recentemente estabelecido, os delegados devem avaliar o seu impacto em outros direitos humanos fundamentais. Especialmente, sugere-se a revisão do artigo 12 da Declaração Universal dos Direitos Humanos.
B. Considerando a necessidade de construção do **RGDP.ONU**, deve-se estabelecer as diretrizes para os seguintes eixos:
    a. Privacidade.
    b. Neutralidade.

c. Inimputabilidade.
d. Segurança.
e. Infraestrutura e controle operacional
f. Ética algorítmica

4 Sugestões para a pesquisa individual

Livros

FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. Petrópolis: Vozes, 2012.

ORWELL, George. **1984**. São Paulo: Companhia das Letras, 2009.

PARISER, Eli. **O filtro invisível**: o que a internet está escondendo de você? Rio de Janeiro: Zahar, 2012.

Sites e Reportagens

Ranking de liberdade na internet (por país)

Como a proposta de neutralidade na rede dos EUA pode afetar o mundo?

Internet e Direitos Humanos

Seremos reféns das tecnologias usadas a serviço da vigilância? (Black Mirror)?

Vídeos e Filmes

BLACK MIRROR. "The Entire History of You" (S01 E03). Dirigido por Brian Welsh. 44 minutos. 2011.

BLACK MIRROR. "White Christmas" (Especial). Dirigido por Carl Tibbetts. 74 minutos. 2014.

PARISER, Eli. O filtro invisível: tenha cuidado com os "filtros-bolha" online. TED Talks, 2011. Disponível em https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles?language=pt-br Acesso em 13 abr. 2019.

SNOWDEN. Herói ou traidor, 2016. Dirigido por Oliver Stone. EUA, Alemanha, França. Disney/Buena Vista, 2016. 1 DVD (2h 15min). Disponível em Netflix.

TECMUNDO. **O que é a tal da Deep Web?** Disponível em https://youtu.be/oQYudKJluvw acesso em 3 abr. 2019.

V DE VINGANÇA. 2005. Dirigido por James McTeigue (132min). EUA, Alemanha, Reino Unido. Warner Bros.

Referências Bibliográficas do Guia de Estudos

AKAMAI TECHNOLOGIES. **Overall DNS Traffic Trends**. 2019. Disponível em https://www.akamai.com/us/en/why-akamai/dns-trends-and-traffic.jsp Acesso em 31 mar. 2019.

ALVES, Marco Antônio Sousa. Panóptico digital e ciberpoder: o poder e o direito na sociedade da informação. In: **Anais do 5º Colóquio Latino-Americano de Biopolítica**. São Leopoldo: Casa Leiria, 2015, p. 493-502.

ALVES, Marco Antônio Sousa. Cidade inteligente e governamentalidade algorítmica: liberdade e controle na era da informação. **Philosóphos**, v. 23, p. 215-257, 2019.

BARBOSA, Guilherme Augusto. SILVA, Maria Helena. Segurança da informação**:** a proteção contra o vazamento de dados e sua importância para as empresas privadas. **Revista Eletrônica e-F@tec**, v. 6 n. 1. Out. 2016. Disponível em: http://revista.fatecgarca.edu.br/index.php/efatec/article/view/105. Acesso em 02 abr. 2019.

BASTA, Alfred; BASTA, Nadine; BROWN, Marly. **Segurança de computadores e teste de invasão**. Tradução de Lizandra Magon de Almeida. 2. ed. São Paulo: Cengage Learning, 2014.

BEZERRA, Arthur Coelho. Privacidade como ameaça à segurança pública: uma história de empreendedorismo moral. **Liinc em Revista**, Rio de Janeiro, v.12, n.2, p. 231-242, nov. 2016.

CAMILO, Cássio Oliveira; SILVA, João Carlos da. **Mineração de dados:** Conceitos, tarefas, métodos e ferramentas. Universidade Federal de Goiás (UFC). 2009. Disponível em http://www.portal.inf.ufg.br/sites/default/files/uploads/relatorios-tecnicos/RT-INF_001-09.pdf. Acesso em 30 mar. 2019.

CANONGIA, Claudia. JÚNIOR, Raphael Mandarino. Segurança cibernética: o desafio da nova Sociedade da Informação. **Parc. Estrat**. Brasília-DF. v. 14, n. 29 p. 21-46, jul.-dez. 2009.

CASTELLS, Manuel. **A sociedade em redes.** Trad. Roneide Majer. 6. Ed. Vol. 1. São Paulo: Terra e Paz, 1999.

COSTA, Johnatan da Silva. SILVA, Jovina da. CRUZ, Maria Auxiliadora Pereira da. Segurança de redes de computadores na internet. **Revista Inova Ação**, Teresina, v. 1, n. 2, art. 6, p. 77-88, jul.-dez. 2012. Disponível em www4.fsanet.com.br/revista. Acesso em 02 abr. 2019.

DELEUZE, Gilles. Post-scriptum sobre as sociedades de controle. Trad. Peter Pál Pelbart. **Conversações**: 1972-1990. Rio de Janeiro: Ed. 34, p. 219-226, 1992.

EMC Digital Universe. **The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things**. 2014. Disponível em https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm. Acesso em 30 mar. 2019.

FRANCO, Deivison Pinheiro; MAGALHÃES, Suyanne Ramos. A *dark web*: navegando no lado

obscuro da internet. **Amazônia em Foco**, Castanhal, v. 4, n. 6, p. 18-33, jan.-jul., 2015.

FREEDON on the Net [FOTN]. **The Rise of Digital Authoritarianism**. Freedom House: Washington, New Yourk, Out. 2018. Disponível em https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf Acesso em 10 abr. 2019.

GOOGLE LCC. **Times per day recorded**. Consumer Survey study. 2016. Disponível em https://surveys.google.com/reporting/survey?hl=en&survey=qvycqkraiwh4jijiqifj2ah4su Acesso: 24 mar. 2019.

GUARDIAN [The]. **Barack Obama and surveillance reform: a story of vacillation, caution and fear**. Disponível em https://www.theguardian.com/us-news/2015/jun/03/barack-obama-surveillance-reform-vacillation-caution-fear Acesso em 31 mar. 2019.

GUIDI, Guilherme. **Modelos regulatórios para proteção de dados pessoais**. 2017. Disponível em: https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf. Acesso em 12 abr. 2019.

LIU, Joyce; SUDWORTH, John. In Your Face: China's all-seeing state. Londres, BBC. 2017. Disponível em https://www.bbc.com/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state Acesso em 5 abr. 2019.

MANZANO, José Augusto. OLIVEIRA, Jayr Figueiredo de. **Algoritmos:** Lógica para desenvolvimento de programação de computadores. 28. Ed. São Paulo: Érica, 2016.

MEDINA, Marco. FERTIG, Cristina. **Algoritmos e Programação:** Teoria e Prática. São Paulo: Novatec Editora, 2006.

MENEZES, Pablo. CARDOSO, Lanay M; ROCHA, Fábio. Segurança em redes de computadores uma visão sobre o processo de *pentest*. **Interfaces Científicas - Exatas e Tecnológicas**. Aracaju. v. 1, n. 2, p. 85-96, Jun. 2015.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS [ONU]. **Declaração Universal dos Direitos Humanos**. 1948. Disponível em http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/por.pdf Acesso: 13 abr. 2018.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS BRASIL [ONUBR]. **Artigo 12: Direito à privacidade**. Textos explicativos. 2018. Disponível em https://nacoesunidas.org/artigo-12-direito-a-privacidade/ Acesso em 23 mar. 2019.

OFFICE of the United Nations High Commissioner for Human Rights [OHCHR]. **Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression** (A / HRC / C / L.20). 2016. Disponível em https://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/32/L.20&Lang=E Acesso em 10 abr. 2019.

PARISER, Eli. **O filtro invisível**: o que a internet está escondendo de você? Rio de Janeiro: Zahar, 2012.

POLIDO, Fabrício B. Pasquot et al. **GDPR e suas repercussões no direito brasileiro**. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2018.

RSF [Repósteres sem Fronteiras]. Classificação mundial da liberdade de imprensa. 2018. Disponível em:

https://rsf.org/pt/classificacao%20 Acesso em 14 abr. 2019.

RUEDIGER, Marco Aurélio. [Coord]. **Robôs, redes sociais e política no Brasil**: estudo sobre interferências ilegítimas no debate público na web, riscos à democracia e processo eleitoral de 2018. Rio de Janeiro, Fundação Getúlio Vargas, 20 ago. 2017, v. 1. Disponível em: http:// dapp.fgv.br/wp-content/uploads/2017/08/Robos-redes-sociais-politica-fgv-dapp_.pdf>. Acesso em: 5 abr. 2019.

SANTOS, Rafael. **Conceitos de Mineração de Dados na Web**. Anais do XV Simpósio Brasileiro de Sistemas Multimídia e Web e VI Simpósio Brasileiro de Sistemas Colaborativos. 2009. Disponível em http://www.lac.inpe.br/~rafael.santos/Docs/WebMedia/2009/webmedia2009.pdf. Acesso em 30 mar. 2019.

STONE, Peter Stone; BROOKS, Rodney; BRYNJOLFSSON, Erik, et al. Artificial Intelligence and Life in 2030. **One Hundred Year Study on Artificial Intelligence**: Report of the 2015-2016 Study Panel, Stanford University, Stanford, CA, September 2016. Disponível em http://ai100.stanford.edu/2016-report. Acesso em 6 abr. 2019.

TANENBAUM, Andrew S. **Redes de Computadores**. Trad. Vandenberg D. de Souza. 4. ed. Rio de Janeiro: Campus, 2003.

TELES, Edson. Governamentalidade algorítmica e as subjetivações rarefeitas. **Kriterion**. Belo Horizonte, n. 140, p. 429-448, ago. 2018.

Agradecimento: Ao professor Marco Antônio Souza Alves (UFMG), pela revisão e pelas preciosas indicações bibliográficas.