tradução brasileira

UNESCO Publishing

Organização das Nações Unidas para a Educação, a Ciência e a Cultura

Direitos humanos e criptografia

Direitos humanos e criptografia

Série da UNESCO sobre Liberdade na Internet

Wolfgang Schulz
Joris van Hoboken

Direitos humanos e criptografia

Tradução brasileira

Por Instituto de Tecnologia e Sociedade do Rio (ITS Rio)

Publicado em 2016 pela Organização das Nações Unidas para a Educação, a Ciência e a Cultura, 7, place de Fontenoy, 75352 Paris 07 SP, França

ISBN 978-92-3-100185-7

Os autores agradecem aos revisores e outras contribuições sobre os relatórios dos países, bem como a assistência de pesquisa.

Revisores:
- Eduardo Bertoni, diretor da Autoridade Nacional de Proteção de Dados da Argentina;
- Deborah Brown, Associação para Comunicações Progressivas (APC), África do Sul;
- Sr. Danilo Doneda, Universidade do Estado do Rio de Janeiro, Brasil;
- Sr. Joseph Lorenzo Hall, CDT (Centro para a Democracia e Tecnologia), EUA;
- Christine Runnegar, Sociedade da Internet;
- Sr. Ben Wagner, Diretor, Centro de Internet e Direitos Humanos, Universidade Europeia, Viadrina, Alemanha.

Contribuições e fontes:
Seda Gürses, Ira Rubinstein, Chinmayi Arun, Sarvjeet Singh, Joshita M. Pai, Eduardo Magrani, Daniel Kahn Gillmor.
Assistência em pesquisas:
Felix Krupar, Tobias Mast, Julian Staben.

Tradução:
Ronivaldo Sales
Flávio Jardim
Ana Lara Mangeth
Gabriella Cantanhede
Eduardo Magrani

A UNESCO agradece pelo apoio do Ministério Federal das Relações Exteriores alemão por realizar esta publicação.

Federal Foreign Office

Ilustração de capa: projeto ©Shuttershock/greiss

Tipografado e impresso pela UNESCO
Impresso na França

Índice

Sumário

Prefácio

Esta publicação segue a nova abordagem da UNESCO para as questões da Internet, conforme endossado em novembro de 2015, por ocasião de sua 38ª Conferência Geral. Os nossos 195 Estados-membros adotaram o Documento Final "*Connecting the Dots"* (Conectando os Pontos), em que 38 opções de ações futuras da UNESCO são estabelecidas; e os princípios da Universalidade da Internet (R.O.A.M.), que defendem uma Internet aberta e acessível baseada em direitos humanos, regida por uma participação multissetorial.

Em consonância com este mandato, a UNESCO se esforça para envolver continuamente as partes interessadas (*stakeholders*) nos processos e fóruns internacionais para promover o entendimento de questões que afetam a liberdade de expressão *online*, como segurança, privacidade, transparência, encriptação, proteção de fontes, discurso de ódio e radicalização na era digital.

A presente pesquisa foi elaborada visando implementar a estrutura da Universalidade da Internet. Em especial, responde à opção recomendada pelo Documento Final "*Connecting the Dots"* no qual que a UNESCO "reconhece o papel que o anonimato e a encriptação podem desempenhar como viabilizadores da proteção da privacidade e da liberdade de expressão, além de facilitar o diálogo sobre essas questões".

Além disso, a pesquisa baseia-se no Relatório do Relator Especial sobre a promoção e proteção do direito à liberdade de opinião e expressão, David Kaye, que foi apresentado ao Conselho de Direitos Humanos em junho de 2015.

A encriptação é um tema importante na atual discussão global sobre governança da Internet. A presente pesquisa debruça-se sobre o assunto e busca delinear uma visão global dos vários meios de encriptação, sua disponibilidade e suas possíveis aplicações no cenário de mídia e comunicações. A pesquisa explica como a implementação da encriptação é afetada por diferentes áreas do direito e da política, bem como oferece estudos de caso detalhados sobre encriptação em jurisdições selecionadas. Analisa em profundidade o papel da encriptação no cenário de mídia e comunicações e o impacto em diferentes serviços, entidades e usuários finais. Com base nessa exploração e análise, a pesquisa fornece recomendações sobre políticas de encriptação que são úteis para várias partes interessadas, as quais incluem sinalizar a necessidade de combater a falta de igualdade de gênero no debate atual e também destacar ideias para melhorar o "aprendizado sobre encriptação".

Esta série emblemática de publicações sobre Liberdade na Internet foi iniciada em 2009, com dois objetivos principais: explorar as mudanças nas questões legais e políticas da Internet; e fornecer recomendações para Estados-membros e outras partes interessadas em promover um ambiente mais propício à liberdade de expressão *online*.

Além de servir como um novo recurso de conhecimento para facilitar o diálogo e a colaboração internacional em questões de encriptação, esperamos que esta nova edição seja valiosa e proporcione conhecimento, opções políticas e recomendações na área de encriptação – para a UNESCO, seus Estados-membros, bem como para a sociedade civil, o setor privado e a academia.

A UNESCO agradece ao Prof. Wolfgang Schulz e ao Dr. Joris Van Hoboken por essa avaliação abrangente e aprofundada. A UNESCO agradece, ainda, aos especialistas internacionais que gentilmente revisaram o rascunho e forneceram suas valiosas contribuições.

Frank La Rue

Diretor Geral Adjunto
da UNESCO

Sumário executivo

Este estudo concentra-se na disponibilidade e no uso de uma tecnologia de particular importância no campo da informação e comunicação: encriptação ou, mais amplamente, criptografia. Nas últimas décadas, a encriptação provou ser especialmente adequada para uso em ambientes digitais. Ela foi implementada de forma abrangente por diversos atores para garantir a proteção da informação e da comunicação, procurando atender a interesses comerciais, pessoais e públicos. Do ponto de vista dos direitos humanos, há um crescente reconhecimento de que a disponibilidade e a utilização da encriptação por atores relevantes são ingredientes necessários para a concretização de uma Internet livre e aberta. A encriptação pode, sobretudo, amparar a liberdade de expressão, o anonimato, o acesso à informação, a comunicação privada e a privacidade. Portanto, as limitações na encriptação precisam ser cuidadosamente examinadas. O presente estudo aborda a relevância da encriptação para os direitos humanos na mídia e no campo da comunicação, e a legalidade das interferências, apresentando recomendações para a prática do Estado e de outras partes interessadas.

Esta publicação explora essas questões no contexto da nova abordagem da UNESCO em relação à Internet. A abordagem foi adotada pelos nossos 195 Estados-membros em novembro de 2015 e tem por fundamentação o Documento Final de uma conferência anterior denominada "*Connecting the Dots*" (Conectando os Pontos). Na prática, isso significa que a UNESCO defende o conceito de "Universalidade da Internet" e os respectivos "princípios ROAM" que dizem respeito a uma Internet baseada em direitos (humanos), aberta e acessível, que seja regulada por uma participação multissetorial.

Na **Seção 2**, o estudo fornece uma visão geral sobre encriptação como um elemento cada vez mais essencial do cenário de mídia e comunicações, fazendo uma distinção entre a encriptação implementada pelos provedores de serviços e a utilizada diretamente pelos usuários finais. O estudo também esclarece a diversidade de propriedades da informação e comunicação que a encriptação pode ajudar a garantir, incluindo confidencialidade, privacidade, autenticidade, disponibilidade, integridade e anonimato.

Na **Seção 3**, o estudo explica como a implantação de tecnologias e soluções de encriptação é afetada por diferentes áreas da lei e política relacionadas à informação, incluindo a lei do comércio eletrônico, lei de proteção de dados e acesso do governo a dados e comunicações. A questão do projeto de *backdoors* de encriptação, sob a ótica do acesso governamental legal, é considerada, assim como o desenvolvimento de

normas em nível internacional, por meio de orientações da OCDE e dos relatórios oficiais dos Relatores da ONU.

A **Seção 4** oferece estudos de caso mais detalhados sobre o estado atual da política de encriptação em jurisdições selecionadas (Alemanha, Estados Unidos, Índia, Brasil e região africana). Esses estudos de caso analisam a política de encriptação vista da perspectiva de uma tipologia geral de restrições à encriptação (por exemplo, controles de exportação), bem como medidas positivas para estimular a disponibilidade e adoção da encriptação (por exemplo, na regulamentação da privacidade de dados). Em nenhuma das jurisdições selecionadas existe uma proibição definitiva acerca do uso de encriptação, mas o grau de liberalização da política de encriptação para uso do setor privado é diferente. Mais especificamente, pode haver uma incerteza significativa sobre o status legal preciso da encriptação, que funciona, de fato, como limitação sobre seu uso. O estudo também discute propostas recentes nos Estados Unidos e em outros lugares que restringiriam a disponibilidade de encriptação segura para usuários da Internet, tendo em vista o acesso do governo à informação e comunicação.

A **seção 5** discute as implicações da encriptação para direitos humanos e mídia, e comunicações. Limitações na encriptação interferem potencialmente no direito à liberdade de expressão e no direito à vida privada, protegidos em âmbito internacional. O estudo promove três perspectivas específicas de preocupação a esse respeito.

Primeiro, a encriptação dá suporte ao requisito de comunicações sem restrições, permitindo que as pessoas protejam a integridade, disponibilidade e confidencialidade de suas comunicações, que seriam vulneráveis se realizadas de outra forma. Esse requisito é uma condição prévia importante para a liberdade de comunicação e precisa encontrar forte reconhecimento em âmbito internacional.

Segundo, quando a política ou legislação provocam limitações na encriptação e suas propriedades de segurança, devem ser observadas as garantias processuais, incluindo o princípio da transparência. Isso é particularmente relevante para a situação na qual os Estados não tomam medidas formais, mas contam com a cooperação de atores privados e da indústria para implantar medidas que afetam a encriptação.

Em terceiro lugar, o estudo observa o importante papel dos provedores de serviços intermediários na proteção da experiência dos usuários em suas plataformas. Especificamente, intermediários *online* não apenas têm o papel de intermediários em relação ao conteúdo e conexão de usuários, mas também um dos intermediários de segurança, considerando que suas práticas e padrões de encriptação são altamente relevantes para o acesso e uso efetivo dessas tecnologias pelo usuário.

A **Seção 6** oferece recomendações como *insights* que podem ser úteis para várias partes interessadas, de forma a abordar adequadamente as questões de direitos humanos envolvidas. As recomendações visam diferentes grupos de partes interessadas e o papel específico que desempenham no sistema geral, incluindo governos, organizações internacionais, comunidade técnica, setor privado, sociedade civil, usuários e academia. Em suas recomendações, o estudo observa a falta de sensibilização para as questões de gênero no atual debate e na política existente em relação à encriptação e à necessidade de abordar a posição das comunidades vulneráveis.

1 Introdução

Contexto do estudo

"A criptografia reorganiza o poder: configura quem pode fazer o quê, a partir de quê."[1]

Vivemos em um mundo onde as tecnologias fazem o papel de intermediário em uma parcela cada vez maior da sociedade. As inovações no campo das tecnologias, serviços e práticas de informação e comunicação continuam a remodelar as relações entre os atores da sociedade. Em virtude de suas capacidades arquitetônicas, essas inovações podem resultar na promoção de valores fundamentais, incluindo o acesso à informação e ao conhecimento, à proteção da privacidade ou à capacidade de se comunicar livremente.[2] As escolhas relacionadas ao projeto tecnológico também podem claramente resultar na erosão ou interferir nesses valores, se energia, tempo e recursos forem insuficientes ou políticas que restrinjam indevidamente seu uso ou implantação forem adotadas. Assim, a tarefa dos formuladores de políticas e outras partes interessadas é considerar o design de arquiteturas e ajudar a garantir a proteção dos valores fundamentais em jogo, no que se refere às infraestruturas tecnológicas. As partes interessadas relevantes também devem reconhecer que essas tecnologias não determinam plenamente o desenvolvimento, uma vez que se incorporam nas práticas sociais. Portanto, estudar o fenômeno mencionado envolve rever as tecnologias, mas sem interromper os esforços nesse ponto.

Este estudo foca nos aspectos de direitos humanos relacionados à disponibilidade e uso de uma tecnologia de particular importância para o campo da informação e comunicação: encriptação ou, mais amplamente, criptografia.[3]

Criptografia é um assunto de longa data no campo da matemática, ciência da

---

1 Phillip Rogaway.The Moral Character of Cryptographic Work. Universidade da Califórnia. Dezembro 2015 http://Web.cs.ucdavis.edu/~rogaway/papers/moral-fn.pdf.

2 Ver, por exemplo, Lessig, Reidenberg; Asscher e outros; Balkin; DeNardis.

3 Ed Felten.Software backdoors and the White House NSA panel report. . Dezembro 2013: "Os dois termos são frequentemente usados como sinônimos, embora "criptográfico" tenha um significado técnico mais amplo. Por exemplo, uma assinatura digital é "criptográfica", mas, sem dúvida, não é tecnicamente "encriptação". https://freedom-to-tinker. com/blog/felten/software-backdoors-and-the-white-house-nsa-panel-report/.

computação e engenharia. Geralmente, pode ser definido como "a proteção da informação e computação mediante o uso de técnicas matemáticas."[4] Nas Diretrizes da OCDE, Encriptação e Criptografia são definidas da seguinte forma:

> "Encriptação" significa a transformação de dados pelo uso de criptografia para produzir dados ininteligíveis (dados encriptados) para garantir sua confidencialidade.
>
> "Criptografia" significa a disciplina que incorpora princípios, meios e métodos para a transformação de dados a fim de ocultar seu conteúdo informativo, estabelecer sua autenticidade, impedir a sua modificação não detectada, impedir o seu repúdio e/ou impedir o seu uso não autorizado.[5]

Desde a década de 1970, a disponibilidade da computação digital e a invenção da chamada "encriptação de chave pública" tornou a encriptação mais amplamente disponível em nossas sociedades. Antes disso, versões robustas de encriptação, ou seja, encriptação de difícil ruptura, eram o domínio dos atores do Estado-Nação. No entanto, nas últimas décadas, a encriptação e as inovações contínuas no campo provaram-se excepcionalmente adequadas ao uso em ambientes digitais.

Técnicas criptográficas têm sido implantadas de maneira ampla por diversos atores, com o intuito de garantir proteção das informações e da comunicação no âmbito pessoal, comercial e no setor público. Técnicas criptográficas também são usadas para proteger o anonimato dos agentes de comunicação e, com isso, a privacidade em geral.

A disponibilidade e o uso de encriptação continuam a provocar debates complexos, importantes e altamente litigiosos sobre políticas legais. Uma primeira rodada de debates, acompanhada de contestações legais e outras formas de contestação em nível nacional e internacional, ocorreu nos anos de 1990. O mundo atualmente encontra-se no meio da uma segunda rodada de debates sobre encriptação em nível nacional e internacional, o que sinaliza que o quadro de políticas existentes em relação à encriptação necessita de uma atualização. A segunda e atual rodada de debates foi provocada por revelações sobre o acesso do governo a informações e comunicação que resultaram dos vazamentos de Edward Snowden para a mídia. Desde então, tem havido um aumento notável na disponibilidade de ferramentas de encriptação de ponta-a-ponta, que estão sendo desenvolvidas e disponibilizadas para os usuários.[6] Encriptação forte é geralmente aceita como uma parte necessária e positiva do panorama de mídia e comunicações. Conforme observa o prefácio das Diretrizes da OCDE para Políticas de Criptografia, é "crítico para o desenvolvimento e uso de redes e tecnologias nacionais e globais de informação e comunicação, bem como o desenvolvimento do comércio eletrônico".[7] A encriptação desempenha um papel fundamental nas estruturas de políticas que promovem a segurança e a integridade da rede. Ainda assim, há declarações e propostas do governo sobre a

---

4 Gürses e Preneel 2016.
5 Diretrizes da OCDE.
6 A encriptação de ponta-a-ponta se refere à aplicação de encriptação em ferramentas e serviços de comunicação, de tal modo que apenas os usuários da ferramenta ou serviço tenham acesso às mensagens de texto simples. Para uma discussão aprofundada, veja a Seção 2.
7 Ver Diretrizes da OCDE.

necessidade de reduzir tal uso e implantação, tendo em vista as potenciais barreiras que poderiam se apresentar para a acessibilidade das agências governamentais. Para os propósitos deste relatório, o foco está principalmente no acesso legal dos atores estatais, em vez do acesso não autorizado de forma mais geral, por exemplo, por *hackers* mal-intencionados. Naturalmente, é relevante o fato de que as restrições relacionadas à encriptação, considerando o acesso por parte do governo, podem gerar graves repercussões negativas sobre a capacidade de impedir o acesso não autorizado de forma mais geral.

Ao mesmo tempo, reconhece-se que a encriptação é especialmente relevante para casos de acesso ilegítimo fora do processo legal, seja por atores estatais ou não estatais, e que podem ser nacionais ou estrangeiros.

Neste contexto, pode-se notar que as partes interessadas do setor também aumentaram significativamente sua implantação de técnicas criptográficas nos últimos anos para aumentar a proteção da informação, as comunicações de seus usuários e promover a confiança em seus serviços. Esse desenvolvimento deve ser mantido em perspectiva. Diferentes estudos sobre encriptação observaram que a adoção onipresente de encriptação de ponta-a-ponta por atores relevantes da indústria é improvável, considerando a dependência de dados do usuário em modelos de negócios.[8] No entanto, a ascensão de serviços comerciais oferecendo encriptação de ponta-a-ponta e os apelos por restrições e soluções, tendo em vista o acesso pelos órgãos de aplicação da lei, estão reforçando a atual rodada de debates em torno do uso de encriptação e do status legal da implantação da criptografia em geral.

Do ponto de vista dos direitos humanos, há uma consciência crescente de que a encriptação constitui uma importante peça do quebra-cabeça para proporcionar uma Internet livre, aberta e confiável. O mesmo se verifica em relação à UNESCO. Na publicação da UNESCO "Os pilares para fomentar Sociedades de Conhecimento inclusivas"[9], a encriptação é discutida e identificada como uma área para ações futuras. O estudo *Keystone* preocupou-se em contribuir para o estabelecimento de uma visão "em prol de uma Internet livre, aberta e confiável que permita às pessoas não apenas a ter acesso a recursos de informação de todo o mundo, mas que também contribua com informações e conhecimento para as comunidades locais e globais".[10] Para avançar na concretização dessa visão, há o reconhecimento "do papel que o anonimato e a encriptação podem desempenhar como facilitadores da proteção da privacidade e da liberdade de expressão", bem como o valor do trabalho da UNESCO "para facilitar o diálogo sobre estas questões".[11] Esta publicação segue a nova abordagem da UNESCO para as questões da Internet, conforme endossado em novembro de 2015, por ocasião de sua 38ª Conferência Geral. Nossos 195 Estados-membros adotaram o Documento Final *Connecting the Dots*, no qual são apresentadas 38 opções para ações futuras da UNESCO; e os princípios da Universalidade da Internet

8 Confira, por exemplo, Soghoian 2009, Van Hoboken e Rubinstein 2014, Berkman Center 2016.

9 Ver http://www.unesco.org/new/en/Internetstudy.

10 UNESCO.Keystones to foster inclusive Knowledge Societies. Paris 2015. http://unesdoc.unesco.org/images/0023/002325/232563E.pdf.

11 Ibid. p. 66.

(ROAM)[12], que defendem uma Internet aberta e acessível baseada em direitos humanos, regida pela participação de múltiplas partes interessadas.

Os atuais e anteriores Relatores Especiais das Nações Unidas sobre a promoção e proteção do direito à liberdade de opinião e expressão também reconhecem a encriptação como um facilitador dos direitos humanos no campo da informação e comunicação. Em seu Relatório de 2013, abordando as implicações da vigilância das comunicações pelos Estados sobre o exercício dos direitos humanos à privacidade e à liberdade de opinião e de expressão, o relator da época, Frank La Rue, concluiu que:

> Os Estados devem abster-se de forçar o setor privado a implementar medidas que comprometam a privacidade, segurança e anonimato dos serviços de comunicações, inclusive exigindo a construção de recursos de interceptação para fins de vigilância do Estado ou proibindo o uso de encriptação.[13]

Seu sucessor, o Relator da ONU David Kaye, recentemente dedicou um relatório específico com o objetivo de avaliar o uso de encriptação e anonimato, para exercer o direito à liberdade de opinião e expressão na era digital e apresentou-o ao Conselho de Direitos Humanos em junho de 2015.[14] Kaye observou que a encriptação e o anonimato merecem um status de proteção ao abrigo dos direitos à privacidade e à liberdade de expressão:

> Encriptação e anonimato, os principais veículos de segurança *online* de hoje, oferecem aos indivíduos um meio de proteger sua privacidade, permitindo-lhes navegar, ler, desenvolver e compartilhar opiniões e informações sem interferência, bem como uma forma de permitir que jornalistas, organizações da sociedade civil, membros de grupos étnicos ou religiosos, aqueles perseguidos em função de sua orientação sexual ou identidade de gênero, ativistas, acadêmicos, artistas e outros exerçam os direitos à liberdade de opinião e de expressão.[15]

O relatório abordou, ainda, a questão da conexão dos direitos humanos, com a legalidade de possíveis interferências e ofereceu recomendações para as atividades do Estado e de outras partes interessadas relevantes.[16]

Objeto da pesquisa, escopo e objetivos do estudo

Diante do exposto, fica evidente que há uma contribuição valiosa que pode ser feita mediante estudos que possam servir como base neutra para uma discussão internacional informada sobre encriptação, como meio de prestar apoio aos direitos humanos no ambiente das mídias e das comunicações. Observa-se, em particular, um imenso valor nas conexões com os debates em andamento, nacional e

---

12 Tanto o Documento Final da UNESCO “Connecting the Dots” e o documento conceitual de Universalidade da Internet constam no Apêndice desta publicação.

13 http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/133/03/PDF/G1313303.pdf?OpenElement

14 http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement

15 David Kaye.Reporto f the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, maio de 2015. http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc.

16 Para mais discussões, veja a Seção 3.

internacionalmente, e ao considerar o papel das partes interessadas do setor. Para promover este objetivo, o presente estudo abordará as seguintes questões-chave:

- Qual é o estado atual da implantação de tecnologias e soluções de encriptação no ambiente de mídias e comunicações, por partes interessadas do setor pertinente e por comunidades de usuários finais em geral? (Seção 2.)
- Como a implantação de tecnologias e soluções de encriptação é afetada por diferentes áreas legislativas e políticas da informação? (Seção 3.)
- Qual é o estado atual da política de encriptação em jurisdições selecionadas entre os cinco continentes, incluindo a região africana, sob a perspectiva de uma tipologia geral de restrições à encriptação e de medidas positivas? (Seção 4.)
- Como a implantação de tecnologias e soluções de encriptação está relacionada à proteção dos direitos humanos no cenário de mídias e comunicações? (Seção 5.)
- Quais opções políticas e ações das partes interessadas podem melhor garantir o respeito aos direitos humanos no contexto da encriptação? (Seção 6.)

Antes de abordar essas questões com mais detalhes, vale a pena dedicar um tempo às definições e ao escopo geral do referido estudo. Em última análise, este estudo preocupa-se com o aprofundamento da discussão sobre o papel de suporte da encriptação na proteção dos direitos humanos, sobretudo em relação ao direito à privacidade e ao direito à liberdade de expressão, conforme protegido em nível internacional. Como visto em relatórios recentes, medidas que garantem o anonimato podem ser observadas para desempenhar uma função semelhante à encriptação ao amparar esses direitos. Mas, para evitar equívocos, o estudo distingue constantemente os valores normativos em questão (isto é, proteção da informação ou comunicação privada, proteção do acesso à informação) e os possíveis meios tecnológicos para proteger esses valores (encriptação, autenticação, ofuscação). Além disso, a presente pesquisa esclarece consistentemente as técnicas criptográficas precisas em questão, considerando a variedade de opções disponíveis.

Encriptação, como definido acima, refere-se a um subconjunto de técnicas criptográficas para a proteção de informações e computação. O valor normativo da encriptação, no entanto, não é fixo, mas varia de acordo com o tipo de método criptográfico usado ou implantado e dependendo dos fins. Tradicionalmente, as técnicas de encriptação (*cypher*) eram usadas para garantir a confidencialidade das comunicações e impedir o acesso a informações e comunicações por terceiros que não fossem os destinatários pretendidos. Este é o uso mais comum da encriptação nos debates atuais sobre o assunto, bem como o foco principal deste estudo. Este é, no entanto, apenas um subconjunto de técnicas criptográficas. A criptografia também pode garantir a autenticidade das partes em comunicação e a integridade dos conteúdos de comunicação, fornecendo, assim, um ingrediente essencial para garantir confiança no ambiente digital. Outro subconjunto de técnicas diz respeito à

proteção de metadados, incluindo a proteção do anonimato dos usuários da Internet e de serviços específicos baseados na Internet.

Assim, este estudo abordará as questões sobre a interface de direitos humanos e encriptação com a seguinte observação em mente: em última análise, o importante não é necessariamente a "encriptação", ou qualquer método criptográfico em particular. O que importa, a partir da perspectiva de direitos humanos, são o estabelecimento e a possível interferência em propriedades de comunicação (e informações) voltadas para o ser humano, como confidencialidade, privacidade, autenticidade, disponibilidade, integridade e anonimato. Métodos criptográficos são importantes. Portanto, interferências em seu uso e implantação devem ser cuidadosamente examinadas, pois tais métodos permitem a garantia técnica dessas importantes propriedades, mesmo em plataformas de comunicação não confiáveis, como a Internet. Por exemplo, enquanto um provedor de acesso à Internet não pode encriptar o tráfego entre usuários finais, os aplicativos de comunicação ainda podem implementar protocolos de encriptação que podem garantir a propriedade de "confidencialidade" de suas comunicações.

A encriptação pode ser usada para melhorar o controle de usuários sobre informações pessoais e de correspondência, sendo esse tipo de uso o objeto do presente estudo. Este estudo prioriza, especialmente, o papel da encriptação conforme usada e implementada por diferentes tipos de serviços e organizações na proteção da segurança de dados do usuário e no apoio aos direitos humanos, além de reconhecer a disponibilidade de ferramentas e aplicativos para usuários finais e a importância de projetos voltados para a comunidade. Nota-se, ainda, que a encriptação pode ser aplicada para causar danos pessoais, impedir que pessoas acessem informações a que deveriam ter acesso ou impedir que pessoas usem ferramentas que deveriam estar a sua disposição. Um exemplo é o uso de ataques de encriptação de dispositivo (*ransomware*), que encriptam o dispositivo de usuários com uma chave mantida pelo invasor, revelada apenas em troca de algum resgate. Outro exemplo é o indevido uso restritivo da Gestão dos Direitos Digitais (*Digital Rights Management* - DRM), de forma a afetar desproporcionalmente o acesso à informação e à comunicação.

Há comunidades que merecem particular atenção ao se discutir as implicações dos direitos humanos relativos à encriptação, como ativistas políticos e jornalistas, bem como as respectivas instituições e organizações de que fazem parte. Ao considerar a questão de quem são os beneficiários de direitos humanos da encriptação, pode-se notar que grande parte do debate sobre encriptação tem ignorado questões de gênero, ou pior, tem sido dominado por homens. É plenamente reconhecido que, sobretudo mulheres e meninas, podem sofrer violações de seus direitos de expressão, privacidade, dignidade e segurança no ambiente *online*.[17] Cabe ressaltar que a encriptação pode facilitar a proteção de mulheres e meninas e comunidades vulneráveis, que notoriamente constituem uma importante área de atuação e investigação adicional para garantir explicações detalhadas sobre o assunto em

[17] Ver, por exemplo, a UNESCO, "que incentiva o combate à violência *online* e *offline* contra mulheres e meninas", 25 de setembro de 2015. Disponível em http://www.unesco.org/new/en/communication-and-information/resources/news- and-in-focus-articles/all-news/news/launch_of_the_broadband_commissions_report (último acesso: 14 de setembro de 2016).

questão. Em geral, o debate social mais amplo sobre direitos humanos e encriptação deve igualmente obter informações das experiências de pessoas submetidas à vigilância orientada e a abusos de direitos humanos pertinentes, incluindo minorias raciais, étnicas e religiosas, jornalistas, blogueiros, mulheres e meninas, comunidades LGBT, etc.[18]

Os que seguiram a discussão em curso sobre encriptação (e a necessidade declarada de restringi-la) não podem deixar de notar uma tendência recorrente para o falso debate. É importante que os benefícios da encriptação sejam colocados em contexto. Os benefícios da encriptação, por si só, podem ser mal interpretados ou podem não fornecer as proteções esperadas no contexto. Encriptar comunicações entre duas partes em comunicação, por exemplo, não impede que qualquer uma das partes que tenha acesso transmita as informações a terceiros. Infelizmente, a encriptação também pode, inadvertidamente, atrair a atenção ou levantar suspeitas, de maneira que prejudique o efetivo usufruto dos direitos humanos, especialmente em situações em que faltam garantias do Estado de direito. Assim, a mera possibilidade de usar encriptação não é, por si só, uma proteção suficiente para se comunicar livremente.

Por outro lado, as premissas relacionadas aos benefícios dos atores do governo em termos do poder de desencriptação das comunicações também merecem um exame minucioso. Primeiro, há sérias questões sobre o desafio técnico de implementar tais poderes. Mesmo assim, as comunicações sobre atos ilegais planejados podem simplesmente passar despercebidas por todos, através de um discurso aparentemente cotidiano e inócuo. Segundo, o papel desempenhado pela encriptação de obstruir o acesso à informação ou comunicação pode ser significativamente exagerado pelos atores interessados. Talvez esteja na natureza matemática da encriptação o fato de que algumas de suas garantias pareçam ser absolutas. Quando necessário, porém, atores estatais e criminosos dispõem de recursos que podem ser utilizados para contornar ou burlar as técnicas de encriptação (explorando deficiências de implementação ou canais secundários), de modo que os recursos e capacidade computacional de certos atores estatais, mesmo com tecnologias avançadas de encriptação, falham em garantir sua proteção. Além disso, mesmo usando ferramentas de comunicação e informação mais seguras, os usuários podem permanecer vulneráveis de várias maneiras. Um exemplo disso foi a forma como invasores usaram o WhatsApp para direcionar usuários a aplicativos inseguros, durante os protestos de Hong Kong no ano anterior.[19] A informação divulgada recentemente nos documentos da Hacking Team ilustra que surgiu um mercado, no qual tais medidas são usadas contra a sociedade civil, jornalistas e ativistas.[20] Esses avanços sugerem que a encriptação é necessária, mas não suficiente para proteger pessoas e informações sensíveis em um mundo conectado em rede. Tais documentos também evidenciam o ritmo acelerado dos avanços em

---

18 Ver, por exemplo, Gürses, S., Kundnani, A. e Van Hoboken, J., 2016.Crypto and empire: the contradictions of conter-surveillance advocacy. *Media, Culture & Society*, 38 (4), pp. 576-590.

19 Jim Finkle.iOS virus targeting Hong Kong protestors – security firm, Reuters, setembro de 2014. Disponível em http://www.reuters.com/article/hongkong-china-cybersecurity-apple-idUSL2N0RV2D320140930 (último acesso: 14 de setembro de 2016).

20 Alex Hern. Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim. *The Guardian*. 6 de julho de 2015. http://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim (acesso: 14 de dezembro 2015).

torno de métodos e tecnologias criptográficas, que devem chamar a atenção para as declarações gerais ou políticas relativas a essas questões.

2 Encriptação no cenário da mídia e das comunicações

A seguir, será apresentada uma visão geral e concisa do estado da arte dos métodos criptográficos relevantes, aplicados ao cenário de mídia e comunicações. O texto se refere a métodos e aplicações criptográficas específicas para possibilitar a elaboração de uma série de distinções importantes, ao mesmo tempo em que se tenta assegurar que permaneça acessível a um público não técnico. É dada uma ênfase especial aos avanços relacionados com a efetiva implementação e o uso de métodos criptográficos por provedores de serviços, bem como com sua disponibilidade prática para indivíduos e profissionais.

Nessas discussões, as duas distinções básicas a seguir são centrais.[21] Primeiro, uma distinção com base no *responsável* pela implementação da encriptação: a encriptação é usada como resultado da escolha de um provedor de serviços ou é implantada por (comunidades de) usuários da Internet? Ao discutir a implementação de ferramentas e tecnologias de encriptação do usuário ou do cliente, é importante ter em mente aquelas comunidades de usuários com necessidades especiais de segurança que são relevantes da perspectiva dos direitos humanos, como os defensores dos direitos humanos, comunidades marginalizadas, jornalistas e outros atores de mídia *online* que praticam jornalismo.

Uma segunda distinção ocorre entre encriptação de ponta-a-ponta e outros métodos similares. Considerando a questão central da possibilidade de obrigar legalmente os provedores de serviços a fornecer acesso às informações do usuário, esta é uma distinção importante quando se olha para as implicações em termos de direitos humanos, especificamente tratando-se da encriptação. Muitas formas de encriptação são implantadas pelos provedores de serviços para proteger as comunicações de forma que se impeça o acesso não autorizado de *terceiros*, mas cujo provedor de serviços que o implementa ainda tenha acesso aos dados relevantes do usuário. Com a encriptação de ponta-a-ponta, nos referimos à encriptação que também impede que *os próprios* prestadores de serviços tenham acesso às comunicações do usuário. A implementação dessas formas de encriptação provocou recentemente um dos maiores debates sobre o tema.

Técnicas utilizadas pelo provedor de serviços para impedir o acesso não autorizado de terceiros

Entre as técnicas criptográficas mais implantadas está a técnica para proteger o

[21] Seguindo o Ira Rubinstein e Joris van Hoboken.Privacy and Security in the Cloud. Revista de Direito Maine 2014, pp. 488 e segs. e Claudia Diaz, Omer Tene e Seda Gürses. Herói ou vilão: O controlador de dados em direito de privacidade e tecnologias, 74 (2013) Ohio State Law Journal, pp. 923 et seq.

canal de comunicação entre usuários da Internet e provedores de serviços específicos contra o acesso não autorizado de terceiros. Essas técnicas criptográficas devem ser executadas em conjunto pelo usuário e o provedor de serviços para funcionar. Isso significa que elas precisam de provedores de serviços, como editor de notícias *online* ou uma rede social, para integrá-los ativamente no projeto e na implementação de serviços. Os usuários não podem implantar essas técnicas unilateralmente; sua implantação depende da participação ativa do provedor de serviços.

Por exemplo, um provedor de serviços de Internet, como um banco eletrônico ou uma biblioteca *online*, pode decidir proteger a comunicação com os usuários. Os provedores de serviços podem fazer isso contando com o chamado padrão TLS (*Transport Layer Security*, ou Segurança da Camada de Transporte). O TLS permite que o provedor de serviços mantenha a comunicação entre o cliente e o servidor em confidencialidade, sem acesso por quaisquer terceiros. Especialmente, permite também que ambos os lados *autentiquem* as partes em comunicação – normalmente, apenas o servidor – e verifica o conteúdo da comunicação para alterações.[22] Quando o TLS está ativado, os usuários podem confiar que estão fornecendo suas credenciais de *login* bancário ao banco verdadeiro. Os leitores que visitam um site de notícias podem confiar que não estão lendo artigos alterados de notícias.

O protocolo TLS, que fica visível para o usuário normal da Internet por meio do cabeçalho HTTPS, é amplamente usado para proteger o comércio *online*, serviços de governo eletrônico e aplicativos de saúde, bem como dispositivos que formam infraestruturas de rede, por exemplo, roteadores e câmeras. No entanto, embora o padrão já exista há quase 20 anos, a maior disseminação e evolução da tecnologia tem sido lenta, aumentando significativamente nos últimos anos.

Tal como acontece com outros métodos e protocolos criptográficos, os desafios práticos relacionados com a implantação adequada, segura e (mais ampla) são significativos e devem ser considerados. Muitos provedores de serviços ainda não implementam o TLS ou não o fazem adequadamente. Muitos servidores podem não oferecer a versão segura do protocolo, ou seja, TLS, por padrão (*default*) ou de forma alguma. Além disso, os servidores podem optar por usar a mesma chave de encriptação por um longo período, em vez de alternar as chaves a cada sessão e descartar as chaves usadas. A última versão, chamada "*perfect forward secrecy*", geralmente é considerada a melhor prática. Tal versão possui a vantagem de que a divulgação de uma chave apenas revela o conteúdo das comunicações para a sessão correspondente. Ainda assim, muitas implementações dependem de chaves de longo prazo.

A encriptação que protege a comunicação entre usuários e serviços de Internet oferece melhorias significativas à privacidade e segurança do usuário perante terceiros maliciosos. As recentes revelações sobre os programas de vigilância em massa trouxeram novamente à tona a realidade de que quando as grandes

[22] Ver também Eitan Konigsburg. EmbracingHTTPS. Novembro de 2014 http://open.blogs.nytimes.com/2014/11/13/embracing-https/ (último acesso: 14 de setembro de 2016).

empresas não protegem as comunicações entre os usuários e seus servidores, as agências governamentais em todo o mundo podem coletar dados de comunicação em massa.[23] Esta situação sofreu alterações substanciais desde então. Muitas empresas já implantaram soluções semelhantes ao padrão TLS para melhorar a segurança de seus serviços em vista do possível acesso não autorizado aos dados.[24] Em alguns casos públicos, isso também incluiu a proteção de dados em trânsito entre centro de dados de provedores de serviços e entre diferentes provedores similares. Os atores da sociedade civil começaram a monitorar publicamente a implantação do TLS em serviços notáveis, como por exemplo EFF (*Encrypt the Web Report* ou "Encriptar o Relatório da Rede").[25] O Google monitora a implantação de HTTPS nos 100 principais destinos da rede em uma seção especial do Relatório de Transparência.[26]

O aumento da implantação do TLS tem sido especialmente valioso para profissionais como jornalistas[27], bem como para a sociedade civil e outras instituições que valorizam comunicações confidenciais com usuários e fontes[28], fornecendo seu conteúdo aos leitores sem sujeitá-los a riscos desnecessários de espionagem e manipulação de conteúdo. A lista de provedores de serviços de destaque que mudaram para HTTPS implica mais de um bilhão de usuários, pois inclui Twitter, Facebook, buscador Google, Gmail, Tumblr e eventualmente também Yahoo!

Há melhorias notáveis na aplicação da encriptação para proteger a comunicação do usuário em relação a terceiros. Ainda assim, pesquisas e investigações demonstram que implantar e manter medidas de segurança não é uma arte que todo serviço *online* esteja disposto ou seja capaz de dominar. Além disso, o aumento do foco no TLS veio à tona em vulnerabilidades de grande escala nos protocolos relacionados; por exemplo, o "*Heartbleed*" e o "*FREAK attack*".[29] O surgimento dessas vulnerabilidades destacou que esforços conjuntos e contínuos em todo o mundo, dentro das comunidades relevantes de especialistas técnicos, são necessários para garantir e manter a segurança das comunicações por meio da encriptação. Iniciativas como o "*Lets Encrypt*" respondem a alguns desses desafios, incluindo a facilidade de implementação.[30]

No contexto das comunicações sem fio, o uso de técnicas criptográficas que protegem as comunicações de terceiros também é importante. Diferentes padrões foram desenvolvidos para proteger as comunicações sem fio: padrões 2G, 3G e 4G

---

23 Internet Architecture Board (IAB). Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement. Agosto de 2015. http://tools.ietf.org/html/rfc7624. Para obter mais informações e aprofundar a discussão, ver Arnbak 2016.

24 Ver também Van Hoboken e Rubinstein. op. cit.

25 Electronic Frontier Foundation. EFF's Encrypt the Web Report. Novembro de 2014 https://www.eff.org/. encrypt-the-Web-report (último acesso: 29 de agosto de 2016).

26 Google, Relatório de Transparência, HTTPS nos Principais Sites, https://www.google.com/transparencyreport/https/ grid/?hl=en.

27 Kevin Gallagher. Why aren't more news organizations protecting their e-mail with STARTTLS encryption? 24 de fevereiro de 2015. https://freedom.press/blog/2015/02/why-arent-more-news-organizations-protecting- e-mail-with-starttls (acessado pela última vez: 29 de agosto de 2016.

28 Para as fontes, um jornalista normalmente quer proteção do anonimato, além de proteger a confidencialidade do conteúdo das comunicações. Isso requer medidas adicionais relacionadas aos metadados.

29 Ver https://freakattack.com (último acesso: 29 de agosto de 2016).

30 Ver https://letsencrypt.org (último acesso: 29 de agosto de 2016).

para comunicação entre telefones celulares, estações-base e controladores de estações-base; padrões para proteger as comunicações entre dispositivos móveis e roteadores sem fio ('WLAN'); e padrões para redes locais de computadores. Versões anteriores de padrões de segurança sem fio apresentaram fraquezas, enquanto que em versões recentes foram feitas melhorias substanciais.[31]

Uma fraqueza comum nesses projetos é que os pontos de transmissão da comunicação sem fio podem acessar todas as comunicações, por exemplo, o provedor de telecomunicações.[32] Essa vulnerabilidade agrava-se quando os protocolos sem fio autenticam apenas os dispositivos do usuário, mas não o ponto de acesso sem fio. Por exemplo, os primeiros padrões de comunicação móvel (GSM) operam de tal modo que apenas os telefones celulares são autenticados, mas não as estações-base às quais os telefones celulares se conectam. Atores mal-intencionados ou agências governamentais podem se aproveitar dessa fraqueza para interceptar comunicações e rastrear usuários móveis em um determinado local, por meio da criação de novas estações-base falsas. Essas estações-base falsas são comumente chamadas de " *IMSI catchers*".[33] [34] [35]

Devido ao uso difundido de redes sem fio em ambientes locais como residências, a questão da segurança sem fio está cada vez mais urgente com o surgimento da "Internet das Coisas" (*Internet of Things – IoT*). A Internet das Coisas refere-se ao desenvolvimento não apenas de computadores, mas também de cada vez mais objetos (e sensores instalados neles, incluindo microfones e câmeras) conectados à Internet. Quando as pessoas se encontram cercadas por objetos do cotidiano que capturam informações ambientais e se comunicam com redes, a presença ou ausência de medidas de segurança e privacidade em sistemas sem fio se torna ainda mais essencial.[36] Como o recente estudo do Berkman Center sobre encriptação menciona, a Internet das Coisas pode abrir novos canais de monitoramento. Isso também implica que "uma incapacidade de monitorar um canal encriptado poderia ser reduzida pela capacidade de monitorar remotamente uma pessoa por meio de outro canal".[37]

As técnicas discutidas acima podem proteger as informações dos usuários em trânsito ou em repouso contra terceiros. As técnicas podem ser aplicadas de maneira diferente em ambos os pontos, ou apenas em um ponto. Há também uma distinção entre "em repouso" em relação a se os dados são armazenados em um dispositivo ou em um servidor local como na nuvem. Dada a vulnerabilidade dos telefones celulares ao furto, por exemplo, uma atenção particular pode ser dada para limitar,

---

31 A GSMMap fornece uma visão geral por país e provedor de telecomunicações sobre a implementação dessas medidas. Ver http://gsmmap.org (último acesso: 29 de agosto de 2016).

32 Gürses and Preneel, 2016.

33 ACLU. Stingray Tracking Devices: Who's Got Them? https://www.aclu.org/map/stingray-tracking-devices- whos-got-them (último acesso: 29 de agosto de 2016).

34 Eric King e Matthew Rice. Behind the curve: When will the UK stop pretending IMSI catchers don't exist? 5 de novembro de 2014. https://www.privacyinternational.org/node/454 (último acesso: 29 de agosto de 2016).

35 Dan Goodin.Low-cost IMSI catcher for 4G/LTE networks tracks phones' precise locations, arsTechnica. 28 de outubro de 2015. http://arstechnica.com/security/2015/10/low-cost-imsi-catcher-for-4glte-networks-track- phones-precise-locations/ (último acesso: 29 de agosto de 2016).

36 Yulong Zou, Xianbin Wang e Lajos Hanzo. A survey on wireless security: technical challenges, recent advances and future trends. Anais do IEEE. Maio de 2015. http://arxiv.org/pdf/1505.07919.pdf.

37 Berkman Center 2016.

inclusive, o acesso prestado pelo serviço. Em geral, isso não exclui a situação em que o provedor de serviços divulga essas informações a terceiros, como outras entidades comerciais ou governos. Em outras palavras, o usuário precisa confiar no provedor de serviços para agir de acordo com seus interesses. Existe ainda a possibilidade de um provedor de serviços ser legalmente obrigado a fornecer informações do usuário ou interferir nas comunicações particulares com determinados usuários. Na seção a seguir, discutimos métodos que garantem que o próprio provedor de serviços não tenha acesso aos *inputs* do usuário. Existem serviços que utilizam especificamente, como estratégia de marketing, o argumento de não terem acesso ao conteúdo da comunicação de seus usuários.

Técnicas utilizadas pelo provedor de serviços que limitam o seu próprio acesso

Os provedores de serviços também podem tomar medidas que restrinjam sua capacidade de acessar informação e comunicação, aumentando assim a proteção dos usuários contra o acesso às suas informações e comunicações. A integridade de tais medidas, também chamadas de Tecnologias de *Privacy Enhancing Technologies (PETs)*, depende de decisões delicadas relacionadas ao *design*, bem como do interesse do prestador de serviços em ser transparente e responsável. As PETs são projetadas para fornecer funcionalidade e, ao mesmo tempo, minimizar os dados do usuário que se tornam acessíveis ao provedor de serviços. Agora os exemplos mais populares podem ser encontrados no mercado de mensagens privadas.

Vale a pena notar, que para muitos desses serviços, o provedor de serviços pode oferecer alguns recursos adicionais (além da capacidade de comunicação); por exemplo, gerenciamento de lista de contatos – o que significa que eles podem observar quem está se comunicando e com quem –, mas tomar medidas técnicas para que não possam ler o conteúdo das mensagens. Isso tem implicações potencialmente negativas para os usuários. Por exemplo, uma vez que o provedor de serviços conecta os usuários que desejam se comunicar usando o serviço, esse também pode, em primeiro lugar, impedir que os usuários se comuniquem.

O panorama atual dos serviços de mensagens privadas é um cenário de rápida movimentação em relação à encriptação que é implantada, em que diferenças muito sutis no *design* podem ter um impacto significativo nas garantias de privacidade de um determinado aplicativo. O WhatsApp do Facebook e o iMessage[38] da Apple são exemplos de uma implementação em larga escala de mensagens privadas. No entanto, para ambos os serviços, a segurança costumava ser projetada de maneira que o Facebook e a Apple pudessem teoricamente ainda ter uma maneira de auxiliar na interceptação de comunicações não encriptadas, explorando os recursos

[38] Apple, Our Approach to Privacy, http://www.apple.com/privacy/approach-to-privacy/.

adicionais oferecidos.[39] [40] Em um sentido muito restrito, isso desqualificou ambos os aplicativos de serem categorizados como provedores de comunicações seguras privadas de ponta-a-ponta. Recentemente, o WhatsApp concluiu a implantação da encriptação de ponta-a-ponta, que agora é o padrão de seus usuários (mais de um bilhão).[41] O WhatsApp conta com o Protocolo de Sinais projetado pela Open Whisper Systems para sua implementação técnica de encriptação de ponta-a-ponta.[42]

Considerando que sutis diferenças técnicas podem ter implicações significativas para a proteção dos usuários, é uma prática comum na comunidade de engenharia de segurança e privacidade exigir transparência e auditorias técnicas para serviços que alegam fornecer garantias de segurança ou privacidade. Alguns serviços foram exemplares nesse aspecto. Por exemplo, o projeto *open source Signal* e a empresa Open Whisper System oferecem encriptação de ponta-a-ponta, podendo ser validada, pois seu código está aberto ao escrutínio público e também está sujeito à revisão de código.[43] Detectadas vulnerabilidades, observa-se uma maior conscientização em relação à necessidade de mais investimento na auditoria de códigos amplamente usados, provenientes da comunidade de software livre e de código aberto.

Além de garantir a comunicação, os provedores de serviços também podem desempenhar um papel na proteção de dados em repouso, utilizando meios que não lhes permitam acessar os dados não encriptados. Muitos usuários precisam gerenciar vários dispositivos, laptops, telefones celulares, unidades de disco, que podem ser perdidos, roubados ou vendidos. Se nenhuma medida adicional for tomada, qualquer pessoa com acesso ao dispositivo poderá extrair informações armazenadas desses dispositivos. Tais vazamentos podem ter consequências significativas para o proprietário do dispositivo, e para todas as outras partes cujas informações foram armazenadas no dispositivo.

Para proteger as informações nos dispositivos, a encriptação autenticada pode ser aplicada. A adoção da encriptação de dispositivos era limitada e poucos usuários são competentes o suficiente ou conscientes da possibilidade de ativá-la. Mais recentemente, grandes empresas, incluindo o Google e a Apple, começaram a aumentar a capacidade de encriptação de dispositivos.[44] Também neste exemplo, as decisões de *design* sobre onde colocar a chave são relevantes: é improvável que o armazenamento de chaves no dispositivo seja eficaz para um adversário que tenha

---

39 Joseph Cox. Apple's iMessage Defense Against Spying Has One Flaw. Wired. 08 de setembro de 2015. http:// www.wired.com/2015/09/apple-fighting-privacy-imessage-still-problems/ (último acesso: 29 de agosto de 2016).

40 Fabian Scherschel. Keeping Tabs on WhatsApp's Encryption. c't. 30 de abril de 2015. http://m.heise.de/ct/ artikel / Mantendo-Tabs-on-WhatsApp-s-Encryption-2630361.html (último acesso: 29 de agosto de 2016, 2015).

41 Ver Cade MetzForget Apple vs. the FBI: Whatsapp just switched on encryption for a billion users. 5 de abril de 2016. Disponível em http://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption- billion-people/.

42 WhatsApp, Visão Geral de Encriptação do WhatsApp, White paper técnico, 4 de abril de 2016.

43 EFF.Secure Messaging Scorecard. Versão em 3 de novembro de 2015. https://www.eff.org/secure-messaging- scorecard (último acesso: 29 de agosto de 2016).

44 Samuel Gibbs. Google can unlock some Android devices remotely, district attorney says. The Guardian. 24 de novembro de 2015, http://www.theguardian.com/technology/2015/nov/24/google-can-unlock-android-devices-remotely-if-phone-unencrypted (último acesso: 29 de agosto de 2016).

ou possa obter acesso ao dispositivo.[45] O caso da encriptação de dispositivos da Apple deve ser salientado, em particular, por ter suscitado um intenso debate público, inclusive internacionalmente, sobre as repercussões para aplicação da lei. O caso amplamente discutido entre a Apple e o FBI sobre a possibilidade de obrigar a Apple a produzir uma solução alternativa para desbloquear o dispositivo ilustrou muitas das complexidades, bem como a falta de entendimento comum entre *sites* nos debates sobre encriptação.[46] Ao passo que as novas medidas podem provocar problemas para agências governamentais em alguns casos, o fato de que os dados do usuário tendem a ser sincronizados com a nuvem alivia tais preocupações.[47]

Os *players* do setor reconhecem que o gerenciamento e a perda de dispositivos são um problema para os usuários e, em vez de dar ênfase à confidencialidade, a continuação de seus serviços mediante a disponibilidade contínua de dados do usuário tende a ser uma preocupação fundamental. Como consequência, os provedores de serviços normalmente abordam problemas relativos à gestão e perda de dispositivos, replicando os dados do usuário na nuvem. Embora o armazenamento de dados na nuvem ajude a garantir a disponibilidade temporal e em vários dispositivos, também aumenta o risco de expor essas informações ao acesso de terceiros por meio de invasões, tornando-as disponíveis para uso e criação de perfil por provedores de serviços. Além disso, quando os dados são armazenados na nuvem, a encriptação autenticada oferece proteção total e efetiva ao usuário sob a condição de que a chave de desencriptação seja armazenada localmente sob o controle do proprietário dos dados, e não na nuvem.

A abrangência dos modelos de negócio que dependem da coleta e processamento de dados do usuário pode ser um obstáculo para a adoção de mecanismos criptográficos de proteção da informação em repouso. Dessa forma, como Bruce Schneier, afirmou:

> "vigilância é o modelo de negócio da Internet. Isso evoluiu para uma arquitetura de vigilância extremamente extensa, robusta e lucrativa. Você é rastreado praticamente em todos os lugares em que navegar na Internet, por várias empresas e corretores de dados (*data brokers*): dez empresas diferentes em um site, uma dúzia em outro."[48]

Como resultado, a encriptação de ponta-a-ponta provavelmente não será aplicada por provedores de serviços comerciais que dependem de *profiling* feito através de dados de usuários encontrados em aplicativos de nuvem. Avanços recentes em técnicas criptográficas, no entanto, tornam possível fornecer alguns serviços "no

---

45 Andy Greenberg. Cops Don't Need a Crypto Backdoor to Get Into Your iPhone.12 de outubro, 2015. http:// www.wired.com/2015/10/cops-dont-need-encryption-backdoor-to-hack-iphones/ (último acesso: 29 de agosto de 2016).

46 Para uma discussão mais aprofundada, consulte as seções 3 e 4.

47 Micah Lee.Apple still has plenty of your data for the feds. The Intercept. 22 de setembro de 2014. Https: // theintercept.com/2014/09/22/apple-data/ (último acesso: 29 de agosto de 2016). Notavelmente, quando os dados são armazenados na nuvem, isso pode apresentar seus próprios problemas para a aplicação da lei ao obter acesso. Ver, por exemplo, o Comitê da Convenção sobre o Cibercrime (T-CY), Acesso à justiça criminal aos dados na nuvem: desafios, Discussão, Estrasburgo, França, 26 de maio de 2015.

48 Bruce Schneier.How We Sold Our Souls - and More - to the Internet Giants. Maio de 2015. https://www. schneier.com/essays/archives/2015/05/how_we_sold_our_soul.html.

domínio encriptado". Por exemplo, usando técnicas criptográficas avançadas, é possível pesquisar dados encriptados: se os termos de pesquisa são conhecidos antecipadamente, pode-se encriptar dados de tal forma que a encriptação seja segura, mas ainda é possível pesquisar o texto encriptado dos termos de pesquisa, um serviço também conhecido como Recuperação de Informações Privadas (*Private Information Retrieval*). Outros avanços mostram que também pode ser possível realizar outras operações em dados encriptados. Esses avanços na chamada "encriptação homomórfica" significam que o provedor de serviços pode executar cálculos em dados encriptados, mas somente o usuário pode desencriptar os resultados.[49]

Finalmente, os métodos criptográficos desempenham um papel fundamental no gerenciamento de identidades *online*. Sistemas de credenciais digitais podem ser usados para permitir transações anônimas, porém autenticadas e contabilizadas entre usuários e provedores de serviços, e podem ser usados para criar sistemas de gerenciamento de identidades que preservem a privacidade.[50]

Encriptação e serviços colaborativos voltados ao usuário final e à comunidade

Uma característica poderosa da Internet é que ela permite aos usuários finais desenvolver aplicativos e utilizações da rede sem ter que cooperar com os provedores de serviços de Internet relevantes. Com relação a essa característica, muitas das ferramentas de encriptação disponíveis não são desenvolvidas ou oferecidas por prestadores de serviços tradicionais ou organizações, mas por especialistas em softwares livres e abertos e nas comunidades de engenharia da Internet. Um dos principais focos dessas iniciativas é produzir *Privacy Enhancing Technologies (PETs)*, que podem ser implantadas de forma unilateral ou colaborativa por usuários interessados – e provavelmente com competência técnica – que estão prontos, dispostos e capazes de cuidar de seus próprios interesses de privacidade quando interagem com provedores de serviços.

Esses PETs incluem aplicativos de encriptação independentes, bem como *add-ons* do navegador que ajudam a manter a confidencialidade das comunicações baseadas na Web ou permitem o acesso anônimo aos serviços *online*. PGP, ou seja, *Pretty Good Privacy*, encriptação para e-mails é um dos exemplos mais conhecidos e mais antigos dessa tecnologia. Os usuários podem utilizar o PGP, instalando software adicional em seus computadores, além do seu leitor de e-mail. As tecnologias nesta categoria são arquitetadas para fornecer encriptação de ponta-a-ponta, bem como outras proteções sem depender de um provedor de serviços centralizado. Em particular, as soluções do lado do cliente, como o software GnuPG, baseado no PGP, são projetadas para permitir remetentes e destinatários a usarem um intermediário não confiável e potencialmente adversário como seu provedor de banda larga, uma rede social ou um serviço de e-mail baseado na Web, sem depender deles para

---

49 Também de Gürses e Preneel. op cit.

50 Claudia Diaz, Omer Tene e Seda Gürses, Hero or Villain: The Data Controller in Privacy Law and Technologies, 74 (2013) Ohio State Law Journal, pp. 923 et seq.

ativar serviços criptografados. Existem também exemplos de comunicações além do e-mail. O Scramble! e o Cryptogram são exemplos de *plugins* para redes sociais que oferecem aos usuários encriptação de ponta-a-ponta de suas comunicações.[51] Por outro lado, tecnologias como registradores de digitação podem interceptar conteúdo conforme inserido antes que a encriptação seja aplicada, deixando, assim, de oferecer proteção. A invasão de sistemas de informação e dispositivos para acessar dados no momento ou após o momento da desencriptação pode ter o mesmo efeito.

Outra categoria de ferramentas para usuários é a utilizada para mensagens instantâneas, que podem ser instaladas pelo usuário. Essas ferramentas integram os chamados protocolos de encriptação *Off-the-Record (OTR)*,[52] e fornecem confidencialidade das comunicações, bem como o *perfect forward secrecy* e a capacidade de negação. *Perfect forward secrecy* minimiza a quantidade de comunicações comprometidas quando uma chave de encriptação é comprometida. Isso é possível ao garantir que a confidencialidade da comunicação ao longo do tempo não dependa do sigilo de uma única chave, mas de várias chaves de sessão descartadas após o uso. A capacidade de negação refere-se à garantia de que, uma vez terminada a comunicação, ninguém – nem mesmo os usuários envolvidos na conversa do bate-papo – pode usar outros meios técnicos para provar se um usuário específico realmente enviou uma mensagem em particular. Essas diferentes propriedades são projetadas para permitir serviços de bate-papo *online* que se assemelham a conversas verbais. Ao ocultar o conteúdo, elas também ajudam a diminuir a capacidade dos provedores de serviços, provedores de conectividade ou governos para censurar as comunicações dos usuários e restringir a liberdade de expressão com base no conteúdo das comunicações. Por exemplo, usando o OTR no chat do Facebook, os jornalistas podem conseguir comunicar seus conteúdos sem sujeitar-se à aplicação de termos de serviço específicos do país e práticas de remoção de conteúdo relacionadas.

Certos PETs requerem colaboração entre diferentes partes para habilitar o serviço. Por exemplo, sistemas de comunicação anônimos como o *The Onion Router* (Tor)[53] são construídos com base na ideia de que os usuários do sistema se unam para oferecer cobertura uns aos outros e, assim, oferecer anonimato.[54] Governos ou outros agentes maliciosos que registram e analisam dados de tráfego em tais sistemas não podem determinar quais dos usuários, no conjunto de anonimato, está associado a uma ação específica e não é capaz de recuperar padrões de comunicação entre usuários (ou seja, o gráfico de comunicação).[55] A subseção a seguir discute essa proteção de metadados com mais profundidade.

Os diferentes PETs discutidos acima não requerem qualquer implementação por provedores de serviços, embora os prestadores de serviços sejam conhecidos por encorajar ou desencorajar seu uso, tornando os serviços interoperáveis ou bloqueando o uso de tais tecnologias. Por exemplo, os provedores de serviços

[51] http://cryptogram.prglab.org (último acesso: 29 de agosto de 2016).
[52] https://otr.cypherpunks.ca (último acesso: 29 de agosto de 2016).
[53] https://www.torproject.org (último acesso: 29 de agosto de 2016).
[54] Para uma discussão da terminologia técnica relacionada ao anonimato, ver Pfitzmann e Hansen, 2005.
[55] Em Diaz, Tene e Gürses. op cit.

podem aumentar a interoperabilidade com usuários de software de navegação anônima, oferecendo acesso através de um endereço "*.onion"*[56] especial*.* Isso aumenta a segurança dos usuários.

As técnicas de *multi-party computation* (MPC) são outro exemplo de soluções colaborativas que permitem às partes, como, por exemplo, várias ONGs com dados sensíveis, fazerem análises de dados sem revelar seus conjuntos de dados entre si. O que todos esses tipos de projeto têm em comum é o fato de que alavancam a encriptação para fornecer garantias de privacidade e segurança na ausência de uma autoridade centralizada confiável.

Finalmente, vale mencionar a aplicação da encriptação nas transações financeiras. Observam-se muitos avanços recentes nas implementações de criptomoedas usando os chamados protocolos *blockchain*. Esses sistemas podem ter muitos benefícios e esses protocolos também podem ser úteis para novas formas de contratos e atestado eletrônico, ajudas úteis quando a infraestrutura legal não está prontamente disponível. Quanto à proteção da privacidade relacionada a pagamentos, é comum o equívoco de pensar que as técnicas criptográficas usadas no *Bitcoin* garantem pagamentos anônimos. Tecnicamente, no entanto, a única proteção oferecida pelo *Bitcoin* é a pseudonimidade.[57]

Proteção criptográfica dos metadados

A disponibilidade de metadados, ou seja, as informações relativas aos dados de usuários e seus comportamentos de comunicação, podem representar uma ameaça particular aos usuários. Por metadados, neste contexto, nos referimos às informações que os provedores de serviços podem observar na prestação de serviços: quando; com que frequência; por quanto tempo; e com quem os usuários estão se comunicando. É possível inferir gráficos de comunicação, bem como padrões comportamentais detalhados de tais dados.[58] Os metadados também podem ser usados para rastrear pessoas geograficamente e interferir na sua capacidade de se comunicarem anonimamente. Conforme observado pelo relatório do Berkman Center, os metadados geralmente não são criptografados de maneira que os tornem inacessíveis para os governos e, portanto, "fornecem uma enorme quantidade de dados de vigilância que não estavam disponíveis antes que as [tecnologias de comunicação pela Internet] se tornassem difundidas".[59]

As ferramentas e soluções que discutimos nas seções anteriores, por si só, não fornecem proteção da análise de tráfego por provedores de serviços aos metadados. Assim, usando um serviço de mensagens encriptadas de ponta-a-ponta, um usuário protege o conteúdo de suas comunicações, mas torna seus metadados de

---

56 Tom Fox-Brewster. O Facebook abre para usuários anônimos do Tor com o endereço .onion. The Guardian. 31 de outubro de 2014. http://www.theguardian.com/technology/2014/oct/31/facebook-anonymous-tor-users- onion (último acesso: 29 de agosto de 2016).

57 Ver Bitcoin is NOT anonymous, http://www.bitcoinisnotanonymous.com/ (último acesso: 14 de setembro de 2016).

58 Ver, por exemplo, Tokmetzis, D. 'How your innocent smartphone passes on almost your entire life to the secret service', 2014. Tradução inglesa publicada em: https://www.bof.nl/2014/07/30/how-your-innocent- smartphone-passes-on-almost-your-entire-life-to-the-secret-service/ (Acesso em 15 de maio de 2016).

59 Berkman Center 2016.

comunicação (quando as comunicações ocorreram e entre quem) disponíveis aos prestadores de serviços. Independentemente de as comunicações serem encriptadas e autenticadas, uma variedade de provedores de conectividade e serviços pode estar em condições de observar tais comunicações encriptadas. Para minimizar a exposição de metadados significativos, talvez seja necessário usar ferramentas de encriptação em combinação com tecnologias que fornecem anonimato de comunicação.

O Onion Router, mais conhecido como Tor, oferece a capacidade de acessar *sites* e serviços *online* anonimamente. O Tor requer uma comunidade de voluntários para executar *proxies* intermediários que canalizam a comunicação de um usuário com um site, para que terceiros não possam observar com quem o usuário está se comunicando. Com o uso de encriptação, cada *proxy* só conhece parte do caminho de comunicação, o que significa que nenhum dos *proxies* pode, por si só, identificar qual usuário ou site está visitando. Do ponto de vista do provedor de serviços, o Tor pode ser considerado como uma ferramenta a favor do cliente, já que os indivíduos podem usá-lo unilateralmente, sem exigir modificações no serviço. Como mencionado, os provedores de serviços podem aumentar a interoperabilidade com o Tor, abrindo o acesso ao seu site por meio de um endereço especial *.onion*.

Quando um usuário acessa um site por meio do Tor, não é possível para o provedor de serviços determinar a identidade do usuário, que é mascarado por trás de uma série de *proxies*. Além disso, não é possível que *sites* vinculem sessões diferentes a um único usuário, desabilitando efetivamente quaisquer recursos de rastreamento. Obviamente, o Tor não protege o anonimato em relação ao provedor de serviços quando o usuário se identifica diretamente ao serviço.

Além de proteger o anonimato, o Tor também é útil quando o ISP do usuário bloqueia o acesso ao conteúdo. Os usuários podem fazer uso do Tor para acessar os *sites* bloqueados: o ISP do usuário pode observar que o usuário está se conectando a um dos *proxies* do Tor, mas eles não podem ver ou bloquear o site com o qual o usuário está realmente se comunicando. Isso é semelhante à proteção que pode ser oferecida por um VPN (*Virtual Private Network*). Por outro lado, os provedores de serviços, como *sites*, podem bloquear conexões provenientes da rede Tor. Pelo fato de determinados tráfegos maliciosos poderem alcançar provedores de serviços como tráfego Tor e por esse poder interferir nos modelos de negócios, os provedores de serviços podem ter um incentivo para fazê-lo. Essa interferência pode impedir que os usuários usem os meios mais eficazes para proteger seu anonimato *online*.

O navegador Tor permite aos usuários ofuscar a origem e os *endpoints* de suas comunicações quando na Internet. Aqui, *ofuscação* se refere à geração automatizada de sinais "falsos" que são indistinguíveis das atividades *online* reais dos usuários, fornecendo aos usuários uma “cobertura” barulhenta sob a qual seu real comportamento de informação e comunicação permanece inobservável. A ofuscação recebeu mais atenção como método para proteger os usuários *online* recentemente.[60] O TrackMeNot é uma ferramenta de ofuscação para usuários de mecanismos de pesquisa: o *plug-in* envia consultas falsas de pesquisa para o

[60] Ver Brunton, Finn e Helen Nissenbaum. *Obfuscation: A User’s Guide for Privacy and Protest*. MIT Press, 2015.

mecanismo de busca, afetando a capacidade de o provedor do mecanismo de pesquisa criar um perfil preciso do usuário. Embora o TrackMeNot e outras ferramentas de ofuscação de pesquisa tenham sido consideradas vulneráveis a certos ataques que permitem que mecanismos de busca façam a distinção entre consultas geradas por usuários daquelas geradas por computadores, é provável que novos avanços na ofuscação desempenhem um papel positivo na proteção de usuários quando a divulgação de informações é inevitável, como no caso de serviços de pesquisa ou baseados em localização. Dada a disponibilidade generalizada de metadados e a possibilidade de usá-los para fazer inferências sobre pessoas e comportamentos dos usuários, é provável que haja mais pesquisas e desenvolvimentos numa melhor junção de métodos de encriptação e ofuscação para proteger os usuários em ambientes digitalmente mediados.

3 Criptografia, lei e direitos humanos: contexto

Esta seção apresenta uma visão geral concisa da maneira pela qual a lei e a política internacionais referem-se a tecnologias de encriptação, sua disponibilidade e sua implantação em serviços ou por usuários. A seção será introduzida fazendo referência à importante discussão acerca do enquadramento da encriptação como um obstáculo ao acesso legal do governo à informação e comunicação. Esse argumento, de que a encriptação impede que importantes agências governamentais ganhem acesso legal à informação ou comunicação relevante para uma investigação em curso resume-se como o "obscurecimento" ("*Going Dark*") do comportamento de comunicação e informação de agentes maliciosos.

A seguir, um breve esclarecimento da posição da regulação sobre encriptação no comércio eletrônico em geral, proteção de dados e política de segurança, bem como o fato de que a encriptação é um assunto de órgãos e estruturas de definição padrão. Isso ajuda a fornecer uma visão mais ampla que esclarece as muitas maneiras pelas quais a regulação é, e de fato, deveria ser, de modo geral, voltada para a promoção, adoção e implantação de encriptação, de forma a estimular seu uso para proteger a segurança e a privacidade, permitir o comércio global, proteger as operações do governo e estabelecer confiança no ambiente digital de forma mais geral.

A seção é concluída com uma breve discussão sobre as normas internacionais com relação à encriptação e a recente atenção ao papel coadjuvante desta para proteger os direitos humanos à privacidade e à liberdade de expressão.

"Obscurecimento" (*Going Dark*) ou "Idade de ouro da vigilância"

Este é o debate sobre encriptação e seu impacto no acesso governamental legal à informação e comunicação que, de forma mais sucinta, levanta a questão sobre a necessidade de restrições à disponibilidade geral de encriptação forte. Isso se deve ao possível obstáculo que ela poderia apresentar na investigação do crime e na proteção da segurança nacional. A ideia de que o acesso efetivo poderia ser bloqueado por encriptação, mesmo quando todas as garantias processuais e fundamentais tivessem sido cumpridas para obter acesso a informações e comunicações, por exemplo, com mandado aprovado pelo Tribunal, que determine a causa provável das evidências relativas a uma investigação específica, levantou preocupações sobre as implicações para os órgãos de aplicação da lei e segurança nacional. Esse foi o caso na primeira rodada de debates sobre a disponibilidade pública de métodos criptográficos fortes nos anos de 1990, e é o caso atual. Isso levou os funcionários de mais alto nível do governo a fazerem declarações sobre o que consideram inaceitável. E isso resultou em várias propostas para restringir a encriptação forte, alegando que haveria obstáculos para o acesso e provocaria um obscurecimento da atividade maliciosa, ou estabeleceria alguma forma de acesso excepcional para autoridades governamentais relevantes.[61] Incidentes recentes de

[61] Ver referências.

terrorismo levaram a novos pedidos de restrições à encriptação,[62] ao passo que certos países, como a Alemanha ou os Países Baixos, assumiram uma posição rigorosa contra as restrições de encriptação na Internet.[63] Em uma declaração conjunta, a Agência Europeia para a Segurança das Redes e da Informação (*European Agency for Network and Information Security* – "ENISA") e a Europol também tomaram uma posição contra a introdução de *backdoors* em produtos de encriptação.[64] Recentemente, os Ministros do Interior da França e da Alemanha afirmaram conjuntamente a necessidade de trabalhar em soluções para os desafios que a aplicação da lei pode enfrentar como resultado da encriptação de ponta-a-ponta, em particular, quando oferecida por uma jurisdição estrangeira.[65]

Este não é o local para propor este debate na íntegra, porém, para os propósitos deste estudo, é importante esclarecer que existe uma concordância significativa na comunidade técnica acerca das desvantagens fundamentais que acompanhariam o acesso excepcional por agências governamentais relevantes, no que diz respeito à segurança que pode ser proporcionada através de métodos criptográficos implementados adequadamente.[66] Além do fato de que muitas propostas são simplesmente inviáveis em termos técnicos ou impossíveis de serem aplicadas de forma eficaz, elas reduziriam a segurança para todos ao criar vulnerabilidades e não conseguiriam alcançar seus objetivos finais.[67] As restrições teriam também efeitos prejudiciais graves na segurança cibernética, comércio e comércio eletrônico.[68]

Assim, o desafio que a implantação da encriptação pode representar para as autoridades policiais e outras agências estatais que buscam acesso a dados e comunicações seguras permanece na agenda sem uma solução fácil.[69] A questão sobre o tamanho real do problema em relação à aplicação da lei, ao estabelecer níveis suficientes de acesso governamental legítimo à informação e comunicação para fins de prevenção do crime, órgãos de aplicação da lei e segurança nacional, *em função da encriptação,* não pode ser camuflada. O especialista norte-americano Peter Swire afirmou, em uma audiência sobre o assunto no Congresso dos EUA, que a situação atual em que os governos se encontram pode ser caracterizada como uma era de ouro para a vigilância.[70] Christopher Kuner, renomado advogado, ao refletir sobre a primeira rodada de debates sobre encriptação e acesso

---

62 Berkman 2016.

63 McCarthy 2016. Sobre a discussão da Alemanha, ver a Seção 4.

64 ENISA e Europol. On lawful criminal investigation that respects 21st Century data protection. Declaração conjunta Europol e ENISA. 20 de maio de 2016.

65 Cazeneuve 2016.

66 Ver, por exemplo, Harold Abelson et al. Keys Under Doormats: mandating insecurity by requiring government access to all data and communications. Julho de 2015. http://www.crypto.com/papers/Keys_Under_Doormats_FINAL.pdf.

67 Bruce Schneier. op. cit.

68 Swire. Ver também Chicago Tribune. Encryption and the terrorists' tracks, disponíveis em http://www.chicagotribune.com/news/opinion/editorials/ct-fbi-terror-encrypt-apple-google-edit-1214-20151211-story.html (último acesso 29 de agosto de 2016); Nicholas Weaver. We think encryption allows terrorists to hide. It doesn't. Dezembro de 2015. https://www.washingtonpost.com/news/in-theory/wp/2015/12/14/we-think- encryption-allows-terrorists-to-hide-it-doesnt.

69 Para discutir sobre os desafios no contexto do crime organizado, ver, por exemplo, Europol 2015, especificamente o Apêndice 1: O debate sobre encriptação.

70 Testemunho de Peter Swire. Audiência do Comitê Judiciário do Senado. "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy". 8 de julho de 2015. Ver também Peter Swire. Encriptação e Globalização. Revista de Direito de Ciências e Tecnologia de Colúmbia, vol. 23 de 2012. http://papers.ssrn.com/sol3/ papers.cfm?abstractid=1960602.

governamental legal nos anos de 1990, afirma que provaram estar errados, ao considerar a percepção geral de que os proponentes da encriptação haviam vencido essa rodada de debates.[71] O Berkman Klein Center For Internet & Society também conclui que não há situação que se possa caracterizar como um obscurecimento.[72] O Centro argumenta que: "A trajetória do desenvolvimento tecnológico aponta para um futuro abundante em dados não encriptados, alguns dos quais podem preencher as lacunas deixadas pelos próprios canais de comunicação que os órgãos de aplicação da lei temem ficar obscurecidos e fora de alcance."[73]

Resumindo, embora haja muitas propostas para interferir na implantação gratuita de encriptação forte, no que se refere ao interesse de segurança pública, quando avaliadas por seus méritos, essas propostas não se sustentam contra um rigoroso escrutínio científico. Além disso, essas propostas deixam de lado um ponto ainda mais essencial, relacionado ao que está em jogo para os usuários. Medidas de segurança mais avançadas são garantidas e necessárias, considerando o cenário de ameaças existente para usuários de comunicações digitais e de computação. Isso se aplica, sobretudo, a usuários com necessidades especiais no que diz respeito à confidencialidade de suas comunicações. Este cenário de ameaça existente, que inclui um amplo conjunto internacional de atores estatais e não estatais, informa o aumento do uso de encriptação forte pelos prestadores desses serviços, no que diz respeito ao interesse dos usuários em serviços e ferramentas que aumentem a proteção de suas informações e comunicações.[74] Desfazer esses avanços para uma melhor segurança seria um sério retrocesso.

Encriptação e a lei: o cenário mais amplo

Uma visão geral de todas as maneiras pelas quais as leis se relacionam com a implantação, o uso e desenvolvimento de protocolos criptográficos está além do escopo deste estudo. Ainda assim, é importante perceber a enorme abrangência de sua aplicação, a fim de esboçar o cenário geral.

A legislação relativa à privacidade e proteção de dados está fortemente relacionada à proteção dos direitos humanos. A quantidade de países com leis de proteção de dados agora é superior a 100.[75] Um dos princípios fundamentais para o processamento justo e lícito de informações pessoais, regulamentadas por tais leis de proteção de dados, é o princípio da segurança. Esse princípio sugere que sejam tomadas medidas de segurança adequadas para garantir a proteção de dados pessoais contra o acesso ilegal de terceiros aos destinatários pretendidos. O novo Regulamento Geral de Proteção de Dados da União Europeia, adotado em 2016, que entrou em vigor em 2018, prevê um avançado conjunto de regras pertinentes à segurança de dados pessoais. A encriptação pode ser uma proteção importante

71 Kuner 2013.
72 Berkman Center 2016.
73 Idem.
74 Ver também a seguinte avaliação de tecnologia para o Parlamento Europeu, que aborda e descreve diversas opções de políticas para lidar com ameaças desproporcionais de vigilância governamental para pessoas físicas http://www.stoa.europarl.europa.eu/stoa/Webdav/site/cms/shared/2_events/workshops/2015/20151208/EPRS_STU(2015)527410_REV1_EN.pdf (último acesso: 14 de setembro de 2016).
75 Greenleaf 2015. Para essa contagem, a introdução de regras sobre segurança foi um critério.

contra violações de dados pessoais, o que pode afetar milhões de pessoas. Além disso, a encriptação é de particular relevância para a implementação de privacidade e proteção de dados "*by design*". Esses princípios, que são cada vez mais aceitos como pilares para a proteção da privacidade e a proteção de dados no século XXI, só podem ser concretizados com inovação e implementação de técnicas criptográficas.

A criptografia também tem sido um ingrediente essencial para estabelecer as condições para o comércio eletrônico na Internet. Os Princípios da OCDE, que serão discutidos mais adiante, foram adotados para assegurar que a política nacional de criptografia não interfira nesse aspecto e garanta as condições também para os desenvolvimentos internacionais no comércio eletrônico.

Um abrangente objetivo da política em relação ao comércio eletrônico, assim como em relação à proteção de dados, têm sido a promoção da confiança no ambiente *online*. Deve-se notar que, sob a perspectiva dos direitos humanos, a promoção da confiança não pode ser um objetivo em si. Em última análise, o que mais importa neste caso não é que as pessoas tenham confiança, mas que exista uma base de conhecimento relativa às medidas tomadas que faça jus aos reais riscos e danos que existem em relação à autonomia e dignidade humana.[76]

Política internacional de encriptação e direitos humanos

O debate político sobre encriptação tem uma dimensão internacional significativa em função da natureza internacional das redes de comunicação e da Internet, bem como das dimensões do comércio, globalização e segurança nacional. De fato, o comércio global e as comunicações em rede tornam tão difícil desvendar as dimensões internacionais das nacionais que as normas de política de encriptação precisam ser acordadas internacionalmente para serem sustentáveis no ambiente online. Reconhecendo isso, as organizações internacionais contribuíram para o desenvolvimento de normas internacionais relacionadas à encriptação, no campo da proteção de dados, política econômica, controles de exportação, governança da Internet e, mais recentemente, sobre o papel coadjuvante da encriptação na proteção dos direitos humanos. A comunidade técnica da Internet, incluindo o IETF, o W3C e a *Internet Society*, também tem feito importantes contribuições para os avanços internacionais relacionados à política de encriptação, por meio de declarações de políticas e padrões.

A Recomendação da OCDE relativa às orientações para a política de criptografia foi adotada em 27 de março de 1997. A OCDE afirma que as revisões realizadas desde sua adoção concluíram que elas continuam adequadas para abordar as questões e os propósitos para os quais foram desenvolvidas.[77] Existem três componentes para essa intervenção política da OCDE, que é principalmente destinada aos seus países-membros: uma recomendação do Conselho da OCDE, Diretrizes para Política de Criptografia (como um Anexo à Recomendação) e um Relatório sobre os Antecedentes e Questões da Política de Criptografia para explicar o contexto das

76 Conforme registra Kaye, "The trend lines regarding security and privacy online are deeply worrying". op. cit. p. 12

77 Diretrizes da OCDE.

Diretrizes e as questões básicas envolvidas na lei de criptografia e no debate de políticas.

O fator determinante da OCDE foi a formulação de políticas pelos Estados-membros relativas ao uso de métodos criptográficos na esfera comercial, que consistiam em criar "obstáculos para a evolução da informação nacional e global e redes de comunicação" e que poderiam "prejudicar o desenvolvimento do comércio internacional".

O Princípio que é mais explícito sobre a conexão com os direitos humanos é o Princípio 5 sobre a Proteção de Privacidade e Dados Pessoais:

> Os direitos fundamentais dos indivíduos à privacidade, incluindo o sigilo das comunicações e a proteção de dados pessoais, devem ser respeitados nas políticas nacionais de criptografia e na implementação e uso de métodos criptográficos.

Tal como nos demais princípios, é dada uma explicação, afirmando: "Os métodos criptográficos podem ser uma ferramenta valiosa para a proteção da privacidade, incluindo a confidencialidade dos dados e das comunicações e a proteção da identidade dos indivíduos. Os métodos criptográficos também oferecem novas oportunidades para minimizar a coleta de dados pessoais, permitindo pagamentos, transações e interações seguras, porém anônimas." Notadamente, o princípio também suscita questões de privacidade e proteção de dados que podem resultar do uso de métodos criptográficos em transações eletrônicas para garantir a integridade dessas transações. Como mencionado, estes "incluem a coleta de dados pessoais e a criação de sistemas para identificação pessoal" e, portanto, garantem medidas de proteção de privacidade necessárias, a serem estabelecidas adequadamente.

As Diretrizes da OCDE para a Proteção da Privacidade e Fluxos Transnacionais de Dados Pessoais fornecem orientação geral referentes à coleta e gerenciamento de informações pessoais, e devem ser aplicadas em conjunto com a legislação nacional relevante ao implementar métodos criptográficos. No que diz respeito ao acesso legal, os princípios exigem uma abordagem equilibrada, deixando aos Estados-membros um espaço considerável para interpretação.

> As políticas nacionais de criptografia podem permitir acesso legal a texto simples ou chaves criptográficas de dados encriptados. Essas políticas devem respeitar os demais princípios previstos nas diretrizes, da maneira mais abrangente possível.[78]

O foco dos princípios foi colocado na facilitação e prevenção de barreiras ao comércio e comércio eletrônico. Refletindo sobre este enfoque, o princípio mais desenvolvido é o que aborda a cooperação internacional. O Princípio da OCDE afirma que:

> Como parte desse esforço, os governos devem remover ou evitar criar, em

[78] A explicação assinala que: "Este princípio não deve ser interpretado como o pressuposto de que os governos deveriam ou não instituir uma legislação que permitisse acesso legal".

nome da política de criptografia, obstáculos injustificados ao comércio.

Como David Kaye resume, no início da era digital, "os governos reconheceram o papel essencial desempenhado pela encriptação na garantia da economia global, utilizando ou encorajando seu uso para proteger números de identidade emitidos pelo Governo, cartão de crédito e informações bancárias, documentos de uso exclusivo de empresas e investigações sobre o próprio crime *online*." O uso de métodos criptográficos no ambiente de mídia e comunicações em outros domínios é menos desenvolvido, e a transformação digital de mídia e comunicações está em um estágio relativamente inicial.

Em seu estudo sobre a visão para a sociedade do conhecimento, a UNESCO, depois de consultar as partes interessadas, identificou a encriptação como um elemento relevante para a política de privacidade e liberdade de expressão. O relatório Keystones defende que "na medida em que nossos dados podem ser considerados representativos de nós mesmos, a encriptação desempenha um papel na proteção de quem somos e na prevenção de abusos do conteúdo do usuário. Permite ainda uma proteção mais intensa da privacidade e do anonimato em trânsito, garantindo que o conteúdo (e às vezes também os metadados) das comunicações seja visto apenas pelo destinatário pretendido."[79] O relatório finalmente reconhece "o papel que o anonimato e a encriptação podem exercer como facilitadores para a proteção da privacidade e da liberdade de expressão", propondo que a UNESCO facilite o diálogo sobre essas questões.

Os Princípios da Necessidade e da Proporcionalidade desenvolvidos e adotados pelos atores da sociedade civil estipulam a proteção da integridade dos sistemas de comunicações como um dos seus 13 princípios.[80] Os princípios em si não fornecem orientação explícita sobre problemas específicos de política criptográfica, como *backdoors* ou restrições à implantação de encriptação.

O recente relatório do Relator Especial da ONU David Kaye fornece o primeiro relato aprofundado da ONU sobre o status de direitos humanos de encriptação e anonimato.[81] O relatório primeiro discute o panorama contemporâneo das ferramentas de encriptação e anonimato. Refere-se ao direito à privacidade como porta de entrada para a liberdade de expressão e de opinião, o direito de manifestar opiniões sem interferência e o direito à liberdade de expressão. Avalia diferentes restrições de encriptação e anonimato, e prevê conclusões e recomendações que criam as condições para uma melhor proteção na prática, bem como maior debate e ação das partes interessadas.

Kaye observa, por exemplo, como a encriptação fornece segurança para que os indivíduos possam "verificar se suas comunicações são recebidas apenas por seus destinatários, sem interferência ou alteração, e se as comunicações recebidas são igualmente livres de intrusão" (ver A/HRC/23/40 e Corr.1, par. 23). Ele esclarece

---

79 UNESCO. Keystones to foster inclusive Knowledge Societies. Paris 2015.

80 Princípios Internacionais sobre a Aplicação dos Direitos Humanos à Vigilância das Comunicações (os "Princípios Necessários e Proporcionais". Disponível em https://necessaryandproportionate.org.

81 David Kaye. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, maio de 2015. http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc.

como a encriptação permite que as pessoas evitem restrições indevidas no que diz respeito ao acesso à informação e ampara a liberdade de expressão e o acesso à informação e ideias, independentemente das fronteiras. Com relação à aplicação do arcabouço jurídico às interferências relacionadas à encriptação, o relatório descreve os requisitos gerais neste contexto e fornece o seguinte:

> […] Uma análise de proporcionalidade deve levar em conta a forte possibilidade de que as invasões na encriptação e no anonimato serão exploradas pelas mesmas redes criminosas e terroristas que as limitações visam deter. Em qualquer caso, "uma justificativa pública detalhada e baseada em evidências" é fundamental para permitir o debate público transparente sobre as restrições que implicam e possivelmente comprometem a liberdade de expressão (ver A/69/397, par. 12).

A principal conclusão do Relatório é que "a encriptação e o anonimato, e os conceitos de segurança a eles inerentes, proporcionam a privacidade e a segurança necessárias para o exercício do direito à liberdade de opinião e expressão na era digital". O relator reconhece que "tal segurança pode ser essencial para o exercício de outros direitos, incluindo direitos econômicos, privacidade, devido processo legal, liberdade de reunião e associação pacíficas e o direito à vida e à integridade física". Em vista das possíveis limitações, o Relatório afirma que "restrições à encriptação e ao anonimato devem ser estritamente limitadas, de acordo com os princípios da legalidade, necessidade, proporcionalidade e legitimidade do objetivo (ver A/69/397, par. 56)". Especificamente, conclui que "desencriptação por decisão judicial […] só pode ser permitida quando resultante de leis transparentes e de acesso público aplicadas unicamente de forma individualizada às pessoas (isto é, não a uma massa de pessoas) e sujeita a uma garantia judicial e à proteção dos direitos processuais dos indivíduos".

As orientações oferecidas pelos princípios da OCDE e as recentes posições do Relator da ONU sobre encriptação afirmam claramente a importância desta para a proteção dos direitos humanos. Embora não respondam definitivamente à questão de saber se um mandado para a encriptação de *backdoors* deve ser considerado incompatível com o direito internacional, apontam nessa direção. Geralmente, a orientação disponível em nível internacional esclarece que quando limitações são impostas à encriptação, garantias relevantes de direitos humanos devem ser rigorosamente observadas. Após uma seleção de estudos por país na Seção 4, a Seção 5 deste relatório discute a aplicação de instrumentos internacionais de direitos humanos sobre liberdade de expressão e privacidade a limitações de encriptação em maior profundidade.

4 Acontecimentos em nível nacional em países selecionados

Com base na literatura,[82] pode-se discernir muitas maneiras pelas quais diferentes

[82] O Relatório da Relatora da ONU sobre Encriptação e Anonimato e as submissões subjacentes contém uma riqueza de informações sobre diferentes limitações e medidas positivas.

leis e políticas afetam a governança regulatória da encriptação. Embora não faça parte do escopo deste estudo promover uma discussão aprofundada sobre todas as diferentes dimensões legais, convém considerar uma tipologia geral de possíveis limitações e medidas positivas gerais em relação à encriptação em leis e políticas relevantes, antes de fornecer vários estudos de caso específicos de países.

Por um lado, há uma grande variedade de possíveis limitações impostas à encriptação. Essas limitações podem equivaler a limitações muito sérias e diretas na encriptação, tais como uma proibição geral de uso da encriptação segura por indivíduos e entidades do setor privado, e a criminalização do uso da encriptação. Podem ainda equivaler a condições sobre o uso de encriptação segura, tais como exigência de registro para certas entidades e finalidades permitidas, bem como obrigatoriedade de licenciamento do governo e controles de exportação. Outras limitações relevantes incluem poderes legais de neutralização (por exemplo, com o uso de vulnerabilidades de segurança que foram constatadas, mas não divulgadas e enfrentadas[83]), poderes de divulgação de chave de encriptação e mandados de desencriptação. Determinados mandados de desencriptação, como um mandado para provedores de comunicações eletrônicas serem capazes de ajudar no acesso legal ao conteúdo das comunicações, de fato, constituem uma proibição do desenvolvimento de soluções de encriptação de ponta-a-ponta por provedores de serviços. Na prática, existe um perigo de que certos pressupostos legais problemáticos sejam anexados ao uso da encriptação, como a suposição de que os respectivos usuários ocultem conduta criminosa. Finalmente, fora das restrições legais, é possível que acordos informais entre o setor público e privado gerem limitações na encriptação segura para os usuários na prática.

Por outro lado, a legislação e a política existentes contêm uma riqueza de medidas positivas que estimulam a adoção de medidas de encriptação por diferentes atores. Conforme mencionado na Seção 3, as leis de privacidade de dados e comércio eletrônico exigem e incentivam a implantação de encriptação e pode-se encontrar requisitos de segurança relevantes na legislação em outros lugares. Além disso, as leis sobre configuração padrão podem facilitar o desenvolvimento de padrões de encriptação e estimular sua adoção em todos os setores. As políticas públicas também podem contribuir positivamente para a encriptação por meio de programas educativos para usuários, apoio financeiro para desenvolvimento de ferramentas e distribuição, e financiamento de pesquisas relacionadas à encriptação nas áreas de matemática, ciência da computação e engenharia.

A seguir, cinco estudos de caso sobre países são examinados no que diz respeito à situação nacional sobre a estrutura legal e política, em relação à encriptação. Os referidos estudos seguem a tipologia geral discutida acima, debatendo limitações e medidas positivas. Esses estudos, particularmente, indagam se há limitações específicas estabelecidas ou em debate quanto ao uso de encriptação no ambiente de mídia e comunicações por usuários e organizações, e/ou se existem medidas positivas tomadas para promover a adoção e uso de encriptação no ambiente de mídia e comunicações. Os estudos aprofundam-se em especificidades acerca de políticas de nível nacional com particular relevância a partir de uma perspectiva internacional. Os países selecionados para esses relatórios são Estados Unidos,

83 Essas vulnerabilidades de segurança também são chamadas de “zero days”.

Índia, Alemanha e Brasil. A seleção baseou-se em geografia e acessibilidade de materiais relevantes. Para a região africana, foi adotada uma abordagem que apresenta informações de diferentes regiões africanas, para superar o desafio de encontrar fontes específicas relevantes suficientes sobre a política de encriptação em determinado país da região. Os estudos de caso abrangem cinco continentes. Os países específicos dentro de cada região também foram escolhidos com base na elaboração relativa da política de encriptação dos mesmos.

Estados Unidos da América

Um debate político amplo, ativo e contencioso sobre encriptação vem ocorrendo nos EUA desde os anos de 1990. Uma primeira rodada de debates e desenvolvimentos, frequentemente chamada de "Guerras Criptográficas", ocorreu nos anos de 1990. Esses debates envolveram a adoção da Lei de Auxílio das Comunicações para a Aplicação do Direito (CALEA), prevendo requisitos para os provedores de telecomunicações e fabricantes de equipamentos para garantir a possibilidade de escutas eficazes.[84] Também envolveu um debate sobre os controles de exportação existentes em produtos de encriptação forte (considerando sua classificação como munição) e uma investigação criminal sobre Phil Zimmermann, ativista e desenvolvedor de software de criptografia para e-mails. Este caso em particular foi abandonado e o debate geral foi resolvido após a liberalização dos controles de exportação sobre a maioria dos produtos comerciais com fortes recursos de encriptação e a transferência desses itens da "*Munitions List*" dos Estados Unidos (USML), administrada pelo Departamento de Estado, para a Lista de Controle de Comércio (CCL), administrada pelo Departamento de Comércio.[85] O Departamento de Comércio dos EUA mantém alguns controles sobre itens no CCL, incluindo registro, revisões técnicas e obrigações de relatórios, e continua impondo licenças e outros requisitos para itens de encriptação confidenciais e vendas desses itens a governos estrangeiros.

Entre os especialistas, as propostas continuaram sendo apresentadas para abordar a questão chamada de '*Going Dark' (*denominada aqui de "obscurecimento"), como resultado da mudança nas comunicações de telecomunicações para serviços de comunicação baseados na Internet. O debate passou a ter mais destaque recentemente, atingindo o nível de várias observações presidenciais sobre o assunto. O debate atual se inflamou após as revelações de Snowden e o aumento bem documentado das medidas de encriptação implantadas por serviços de Internet, dispositivos e usuários, bem como de um apelo conjunto da comunidade técnica e sociedade civil para aumentar o uso de encriptação e segurança para fazer frente às práticas de vigilância em massa.[86] A crescente adoção da encriptação pelo setor

---

84 Pub. L. No. 103-414, 108 Stat. 4279, codificado em 47 USC 1001-1010)

85 Ver EUA Departamento de Comércio, Controles de Exportação de Encriptação: Revision of License Exception ENC and Mass Market Eligibility. Junho de 2010. Ver também Ira Rubinstein e Michael Hintze. Controles de Exportação no Software de Encriptação. http://encryption_policies.tripod.com/us/rubinstein_1200_software.htm (último acesso: 14 de setembro de 2016).

86 Ver Ira Rubinstein e Joris van Hoboken. Privacy and Security in the Cloud, Maine Law Review 2014. O debate particularmente sobre encriptação já se realizava antes das revelações de Snowden, como agentes dos órgãos policiais dos EUA defendiam a extensão das obrigações de escuta telefônica

industrial foi recebida de forma crítica por certos atores do governo, o FBI em particular. Eles engendraram uma disputa legal amplamente divulgada entre a Apple e o FBI sobre a possibilidade de obter acesso a informações sobre o iPhone como suporte à aplicação da lei.[87] Em 2016, vários projetos de lei foram apresentados no Congresso dos EUA, que estabeleciam novos limites de encriptação nos termos da legislação dos Estados Unidos.

Em geral, o sistema legal dos EUA promove e exige que medidas de segurança sejam implementadas nos contextos relevantes, incluindo métodos criptográficos de vários tipos, para garantir a segurança nas relações comerciais. Uma visão geral de tais leis ultrapassa o escopo deste relatório de país, mas a legislação dos Estados Unidos prevê diversas leis que promovem e impõem métodos criptográficos. A legislação pertinente se constitui na Lei Federal de Modernização da Segurança da Informação (FISMA) de 2014, na Lei *Gramm-Leach-Bliley*, na Lei de Portabilidade e Responsabilidade de Seguro de Saúde (HIPAA) e também na Lei da Comissão Federal de Comércio. Tais normas preveem requisitos de segurança e, portanto, exigem ou estimulam indiretamente o uso da encriptação em determinadas circunstâncias. Por fim, muitas leis estaduais de notificação de violações tratam os dados criptografados como um porto seguro, ao isentar das obrigações de notificação as empresas que tenham utilizando encriptação de dados.

O amparo para a implantação e uso de métodos criptográficos igualmente se estende ao contexto internacional, em que os EUA estão entre os principais defensores da coordenação internacional. O governo dos EUA apoia a pesquisa e o desenvolvimento de métodos e padrões criptográficos mediante iniciativas de financiamento departamental, bem como pela Fundação Nacional da Ciência. Por fim, a Agência de Democracia, Direitos Humanos e Trabalho (DRL) do Departamento de Estado dos EUA financia diversos projetos relacionados à liberdade na Internet, com o intuito de "promover as liberdades fundamentais, os direitos humanos e o livre fluxo de informações online, incluindo financiamento do governo para soluções de encriptação forte para fazer frente às restrições e limitações no acesso a informações online.[88]

Considerações constitucionais e direitos humanos desempenham um papel fundamental no debate dos EUA sobre o tratamento legal de métodos de encriptação. Restrições à distribuição de protocolos criptográficos e à publicação de métodos criptográficos constituem uma interferência à Primeira Emenda, a garantia constitucional dos EUA que protege a liberdade de expressão. Especificamente, o Nono Tribunal de Recursos decretou que o código-fonte do *software* constitui um

(CALEA) para serviços de Internet. Para debater sobre o assunto, ver Adida et al. 2013.

87 Eric Geller 2016.

88 Para avaliar os projetos financiados e a eficácia do programa, ver Ryan Henry, Stacie Pettyjohn e Erin York. Avaliação de Portfólio do Programa de Liberdade na Internet no Departamento de Estado. RAND National
Divisão de Pesquisa de Segurança. Fevereiro de 2014
http://www.rand.org/content/dam/rand/pubs/working_papers/ WR1000/WR1035/RAND_WR1035.pdf. Um estudo mais recente avalia a questão de saber se tais projetos poderiam beneficiar o uso ilícito Sasha Romanosky, Martin C. Libicki, Zev Winkelman, Olesya Tkacheva. Software de Liberdade na Internet e Atividade Ilícita, Apoiando os Direitos Humanos sem Permitir a Ação de Criminosos. Rand Corporation. 2015. http://www.rand.org/pubs/research_reports/RR1151.html.

discurso protegido pela Primeira Emenda e que os regulamentos do governo que restringiam sua publicação eram inconstitucionais.[89] Além disso, a legislação e a política dos EUA sobre encriptação são rigorosamente informadas em função da competitividade daquele país (para empresas norte-americanas de grande sucesso operarem no exterior e terem acesso e excelência em mercados relacionados a serviços de Internet), bem como os interesses legítimos de acesso do governo relacionados à aplicação da lei, segurança nacional e à comunidade de inteligência. Um terceiro fator que implica significativamente em política de encriptação é o objetivo de proteger a infraestrutura crítica dos EUA.

Os EUA dispõem de agentes da sociedade civil particularmente ativos e fortemente desenvolvidos, envolvidos em políticas e práticas de encriptação. O país é um local fundamental para a pesquisa e engenharia de criptologia, desenvolvimento e implementação de inovações de serviços criptográficos. Adicionalmente, existe uma grande comunidade de Organizações Não Governamentais dedicadas ao debate nacional e internacional sobre política de encriptação.[90]

As interferências predominantes na encriptação forte, que são efetuadas ou que estão sendo consideradas, ocorrem no campo da segurança nacional, aplicação da lei e relações internacionais. Nessa área e na resposta à questão contenciosa da condição e da maneira como o acesso legal a comunicações específicas poderia ser assegurado, o governo dos EUA explicou internacionalmente sua política que visa assegurar que “encriptação implantada com responsabilidade" ajuda a "proteger muitos aspectos de nossa vida diária, incluindo nossas comunicações e comércio privados", mas também para “garantir que os agentes maliciosos possam ser responsabilizados sem enfraquecer nosso compromisso com a encriptação forte”.

Algumas especificidades estão disponíveis sobre a forma como este difícil equilíbrio é atualmente atingido na prática nos EUA, nas seguintes modalidades (além da possibilidade de que evidências suficientes possam ser obtidas fora do âmbito da informação e comunicação potencialmente encriptadas):

Disposições de assistência técnica

Nos casos em que são atendidas as condições para o acesso legal a informações ou comunicações, a legislação dos EUA, assim como outros sistemas jurídicos, determina obrigações aos prestadores de serviços pertinentes no que diz respeito a prestar assessoria jurídica na produção de informações ou comunicações relevantes solicitadas pelas respectivas autoridades. Como já mencionado, a CALEA impõe exigências ao setor de telecomunicações para garantir que os prestadores de serviços possam ajudar nas interceptações de telecomunicações. A Lei de Privacidade das Comunicações Eletrônicas exige que os provedores de serviços e outras determinadas entidades forneçam “todas as informações, instalações e suporte técnico necessários para se realizar a interceptação de forma discreta e com um mínimo de interferência” nos serviços que o provedor estiver prestando para o

89 Bernstein vs. Departamento de Justiça dos EUA, Nono Tribunal. Decretou: 6 de maio de 1999.
90 Ver, por exemplo, a Encrypt all the Things Campaign.

indivíduo-alvo".[91] Mais recentemente, o FBI testou os limites da *All Writs Act* (Lei de Todos os Mandados) para ser aplicada como a fundamentação de mandados judiciais aos prestadores de serviços, de forma a burlar o acesso aos dispositivos. A disputa judicial amplamente divulgada entre a Apple e o FBI é o exemplo mais conhecido desta nova linha de casos, mas petições similares foram apresentadas em tribunais diferentes em várias partes dos Estados Unidos.

Cooperação informal

O arcabouço jurídico dos EUA oferece uma variedade de proteções legislativas, constitucionais e regulatórias que asseguram a proteção de dados e comunicações do usuário contra o acesso indevido pelo governo. A legislação dos EUA realmente oferece espaço jurídico para a cooperação voluntária e acordos informais entre empresas e agências governamentais, inclusive para garantir a cooperação ideal em investigações criminais e questões de segurança nacional. A ECPA prevê determinadas restrições à divulgação voluntária em relação aos serviços cobertos, mas elas envolvem a produção de dados e não a cooperação no que diz respeito à capacidade de produzir tais dados. Geralmente, as garantias constitucionais dos EUA não se aplicam em casos de cooperação voluntária por falta de ação do Estado.[92] Altos funcionários da comunidade de inteligência esclareceram que um dos impactos mais significativos das recentes divulgações sobre a vigilância do governo tem sido a crescente falta de vontade dos principais *players* industriais para continuar a cooperar voluntariamente.[93] Internacionalmente, o governo dos EUA se encontra em uma posição única em comparação com outros Estados, uma vez que muitas das empresas de Internet mais bem-sucedidas internacionalmente estão sediadas no país.

---

91 Para discutir o assunto, ver []. A FISAAA 2008 (Lei de Emendas de 2008 à Lei de Vigilância Internacional de 1978) contém linguagem ligeiramente diferente, exigindo que a assistência permaneça oculta ao usuário. Além disso, os tribunais podem lançar mão de disposições gerais da Lei de Todos os Mandados ("All Writs Act") para solicitar assistência. Para discutir sobre um caso recente, ver Jennifer Granick. Juiz Federal chama a atenção para o debate sobre o "Going Dark". O Centro para Internet e Sociedade. Outubro de 2015. http://cyberlaw.stanford. edu/blog/2015/10/federal-judge-shines-spotlight-%E2%80%9Cgoing-dark%E2%80%9D-debate (último acesso: 14 de setembro de 2016).

92 Comparar Derek Bambauer. Poltrona de Orwell. Revista de Direito 79 da Universidade de Chicago (2012), 3, pp. 863-944. https://lawreview.uchicago.edu/sites/lawreview.uchicago.edu/files/uploads/79_3/01%20Bambauer%20ART.pdf (último acesso: 14 de setembro de 2016). Ver também Solove 2002.

93 Ver Wilson Center Symposium.How have we changed? Evolving Views in the U.S. on Security and Liberty. Comentários de Bob Litt, https://www.youtube.com/watch?list=PLzM1iiQhV r dHHZPSZ1z_ ztTrUuRPMUtRb&v=PWj8eqKKB64 ("Há uma longa história de relacionamentos cooperativos entre empresas americanas e governo americano no interesse de proteger a nação e seus cidadãos. [..] As empresas não foram solicitadas a agirem ilegalmente em quaisquer circunstâncias. Elas contam com advogados próprios, que são bem qualificados em proteger seus próprios interesses. Mas como se observou a existência de lacunas tecnológicas que a NSA procura preencher, existem lacunas legais. Pode haver uma área de espaço entre o que é especificamente autorizado por estatuto e o que é especificamente proibido por lei e, em seguida, há uma zona cinzenta, onde temos tido muito sucesso ao longo dos anos ao assegurar cooperação voluntária. Parece ter sido uma perda inquestionável para a nossa capacidade de proteger a nação, se as empresas pretendem suspender esse tipo de cooperação voluntária."). Ver também Michaels, Jon D., All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror (6 de outubro de 2008). California Law Review, vol. 96, p. 901, 2008. Disponível no SSRN: http://ssrn.com/abstract=1279867.

Violação e quebra de proteção

Finalmente, a encriptação de dados armazenados ou transmitidos, mesmo quando implementada e executada corretamente, pode ser violada ou burlada por autoridades competentes para garantir o acesso legal a informações e comunicações, sem o envolvimento de um usuário ou provedor de serviços. Por exemplo, autoridades relevantes podem obter acesso a informações não encriptadas em dispositivos do usuário final com a instalação de *key loggers* ou outros meios, como ataques de canais laterais. Estes poderiam aproveitar as falhas de implementação em software criptográfico e implementações. Intensos debates vêm sendo travados sobre as formas pelas quais ocorrem a exploração de vulnerabilidades de softwares (chamadas de "*zero-days*"), pois ao invés de corrigirem as inseguranças, acabam por prolongá-las aos usuários da Internet de maneira geral. Finalmente, a mais controversa das opções acima tem sido a interferência documentada na segurança dos padrões criptográficos em contextos de configurações padrão. Isso levou a reações de profunda preocupação por parte da comunidade técnica[94], e especialistas internacionais questionaram a falta de separação de recursos relacionados à capacidade de encriptação ofensiva da garantia de informações em agências relevantes dos EUA.[95] Especificamente, a preocupação é que a missão de garantir a segurança defensiva seja prejudicada por aqueles, na mesma agência, focados em capacidades ofensivas. A regulamentação legal e o escrutínio constitucional, de acordo com a legislação dos EUA, sobre o uso de métodos distintos com o objetivo de violar ou quebrar a segurança da encriptação, ainda está no começo.

Considerando essas diferentes opções e os vários desafios a elas associados, o cenário dos EUA, nesse aspecto, continua sendo altamente dinâmico, e altos funcionários da comunidade de aplicação da lei e de inteligência exigiram garantias adicionais para assegurar o acesso a comunicações e informações não encriptadas. Estas propostas são variadas, incluindo a extensão dos requisitos da CALEA, atualmente aplicáveis apenas a serviços de telecomunicações (incluindo telefones celulares), a serviços de Internet, requisitos de custódia de chaves,[96] chaves de ouro[97], bem como proibições definitivas da funcionalidade de encriptação de ponta-a-ponta. Até o momento em que o presente relato foi redigido, a posição da Casa Branca foi moderadamente contrária à introdução de novos requisitos regulatórios. Um projeto de documento político da Casa Branca, que foi publicado pelo *Washington Post*, esclarece que a mesma geralmente considera negar ou adiar a

---

94 Ed Felten. On Security Backdoors. Freedom to Tinker. 11 de setembro, 2013. https://freedom-to-tinker.com/blog/felten/on-security-backdoors/; Neal Koblitz and Alfred Menezes. A Riddle wrapped in an Enigma. Dezembro 2015 http://eprint.iacr.org/2015/1018.pdf; Daniel Bernstein, Tanja Lange and Ruben Niederhagen. Dual EC: A Standardized Back Door. Cryptology ePrint Archive: Relatório 2015/767.

95 Amir Mizroch, Surveillance and Silicon Valley Are 'Destroying' Europe's Privacy Balance. 11 de dezembro de 2015. http://blogs.wsj.com/digits/2015/12/11/surveillance-silicon-valley-destroying-europes-privacy- balance.

96 A custódia de chaves envolve requisitos que as chaves de encriptação sejam armazenadas por terceiros, de modo a estarem disponíveis em caso de pedidos legais de acesso do governo.

97 "Golden key/chave de ouro" é outro termo que foi usado para a criação de uma backdoor para segurança de encriptação. A proposta chave de ouro implica a criação de um backdoor seguro, cuja chave só é conhecida pelas partes autorizadas. A possibilidade de criar soluções seguras de chave de ouro é contestada pela comunidade técnica.

introdução de uma determinada legislação.[98] O referido documento demonstra também que as rotas informais disponíveis para garantir níveis ótimos de acesso governamental legal, do ponto de vista da aplicação da lei e da segurança nacional, continuam sendo considerações centrais.

Alemanha

Como parte do debate global sobre encriptação no final da década de 90 , houve um debate na Alemanha sobre a necessidade e legitimidade da imposição de uma proibição geral da encriptação das comunicações devido ao impacto nas investigações criminais.[99] Ao contrário, por exemplo, do Reino Unido, onde uma proibição semelhante já não é considerada seriamente.[100] Há profundas dúvidas sobre a legitimidade constitucional, bem como preocupações sobre as consequências factuais negativas de tal proibição.[101] Em termos qualitativos, vários direitos fundamentais são afetados por restrições de encriptação: o sigilo das telecomunicações, a expressão do direito geral de personalidade e, indiretamente, todas as liberdades comunicativas que são exercíveis por meio da Internet.[102] Foi por isso que o Governo Federal estabeleceu aspectos-chave em 1999 para a política de criptografia alemã, que devem garantir confiança especialmente na segurança da encriptação em vez de restringi-la.[103]

De modo geral, e além das declarações do Ministro do Interior alemão sobre possíveis restrições futuras, a Alemanha alinha-se com a posição do Relator Especial da ONU David Kaye e adota políticas de não-restrição ou proteção abrangente e somente adota restrições em casos específicos.[104] Na apresentação para David Kaye, esclarece-se que a estratégia alemã de segurança cibernética trata de garantir a segurança de empresas e particulares na Internet. O Governo Federal encoraja e apoia, portanto, o uso da tecnologia de encriptação.[105]

Neste sentido, muitas discussõesvêm ocorrendo para definir se uma chave mestra para agências de segurança (*backdoor*) é ou não sensata e viável. O debate também reconheceu a disponibilidade e a possibilidade de soluções mais direcionadas ao discutir regimes jurídicos de acesso que não sejam direcionados para algoritmos de encriptação em si, mas tendam a ser direcionados para espionagem de senhas e chaves usando *software* "*sniffer*" ou "*keyloggers*".[106] Existe uma crescente jurisprudência sobre esses meios de acesso do governo aos dados e sobre as garantias exigidas com base na Lei Fundamental Alemã (Constituição).[107]

---

98 NSC apresenta um documento de opções sobre abordagens estratégicas para encriptação. Verão de 2015 <http://apps. washingtonpost.com/g/documents/national/read-the-nsc-draft-options-paper-on-strategic-approaches- to-encryption/1742/>.

99 Alexander Koch. Grundrecht auf Verschlüsselung?. CR 1997, p. 106.

100 Gerrit Hornung. Die Krypto-Debatte: Wiederkehr einer Untoten. MMR 2015, 145 et seq.; Kuner/Hladjk in Hoeren/Sieber. Multimedia-Recht. part 17, recital 62 et seq.

101 cf. Koch op cit. p. 108 et seq.

102 Ver Julia Gerhards. (Grund-)Recht auf Verschlüsselung?. 2010. p. 123 e seguintes.

103 Kuner/Hladjk in Hoeren/Sieber Multimedia-Recht. parte 17, recital 64.

104 David Kaye. op cit. § 57.

105 Apresentação ao Relator Especial da ONU, David Kaye, sobre o status legal da tecnologia de encriptação na Alemanha.

106 Gerhards op cit. p. 409

107 Referência cruzada à discussão da jurisprudência mais adiante.

A população alemã é normalmente mencionada internacionalmente por atribuir um peso especial ao direito à privacidade e à proteção de dados pessoais. A Alemanha pode, assim, ser notável na atitude geral da população em relação à proteção da privacidade e das garantias relacionadas. Uma pesquisa conduzida pela BITKOM na Alemanha mostrou que o número de entrevistados que encriptam seus e-mails aumentou de 6%, em 2013, para 16%, em 2014. Embora a pesquisa de 1000 entrevistados possa não ser representativa, a tendência por mais encriptação é reconhecível.[108] Existem vários nichos para serviços de comunicação encriptada e projetos de desenvolvedores ativos na Alemanha, como o provedor de e-mail alemão Posteo, que visa estabelecer novos padrões para gerir os dados de seus usuários.[109]

Existe, por exemplo, o serviço de mensagens de Internet, Telegram, com sede em Berlim, que recentemente causou um tumulto devido a rumores de que os membros do ISIS estariam usando o serviço.[110] O Gpg4win (GNU Privacy Guard for Windows), um software de encriptação para arquivos e e-mails, é outro exemplo vinculado aos desenvolvedores alemães. Pode-se dizer que, como resultado dos vazamentos de Snowden, uma nova geração de startups cresceu na Alemanha.[111]

Em novembro de 2015, representantes governamentais e representantes do setor privado assinaram um "Termo para fortalecer a comunicação confiável" (*Charta zur Stärkung der vertrauenswürdigen Kommunikation*) em conjunto, no qual eles declaram: "Queremos ser o site de encriptação número 1 no mundo".[112] Ao contrário de outros lugares, em nível europeu ou nos Estados Unidos, os recentes ataques em Paris não suscitaram um novo debate nacional sobre encriptação.[113] O Escritório Federal Alemão de Segurança da Informação forneceu novas diretrizes sobre a implementação de padrões de e-mail, endossando novos padrões técnicos da IETF para e-mails seguros.[114] O governo alemão também usou sua política externa para promover padrões internacionais de privacidade. Em particular, a Alemanha, em um esforço conjunto com o Brasil, comprometeu-se no Conselho de Direitos Humanos para a nomeação de um Relator Especial da ONU de Privacidade.[115]

---

108 Pesquisa BITKOM 08/2014. Cybercrime. https://www.bitkom.org/Presse/Anhaenge-an-PIs/2014/August/140827-BITKOM-Charts-PK-Cybercrime-mit-BKA-28-07-14.pdf.

109 Ver Michael Scaturro, Protect your email the German way, The Guardian, 24 de agosto de 2016,https://www. theguardian.com/technology/2014/aug/24/posteo-protect-email-the-german-way-patrik-lohr (último acesso: 14 de setembro de 2016).

110 Markus Böhm. Messenger Telegram: Lieblings-App der IS-Terroristen sperrt Propagandakanäle. 18 de novembro2015.http://www.spiegel.de/netzwelt/apps/is-auf-telegram-messenger-app-kuendigt-massnahmen-an-a-1063535.html.

111 Isabelle de Pommereau. In Snowden's wake, crypto-startups take root in Germany. 3 de agosto de 2015. http:// www.csmonitor.com/World/Passcode/2015/0803/In-Snowden-s-wake-crypto-startups-take-root-in-Germany.

112 Digital Agenda 2014-2017, p. 33.

113 Ver Fabian Warislohner. Tatort: Verschlüsselung. Die Schuldfrage nach Paris. 19 de novembro de 2015. https:// netzpolitik.org/2015/tatort-verschluesselungstechnik-die-schuldfrage-nach-paris. Mas, ver Cazeneuve 2016 referente a um apelo conjunto recente para a ação do Ministro do Interior alemão e seu correspondente francês.

114 Richard Chirgwin, German infosec bureaucrats want mail providers to encrypt, The Register, 21 de outubro de 2015,http://www.theregister.co.uk/2015/10/21/german_infosec_bureaucrats_want_mail_providers_to_encrypt/ (último acesso: 14 de setembro de 2016).

115 Ver Monika Ermert, NSA-Skandal: UN-Sonderberichterstatter für Datenschutz in der digitalen Welt angestrebt, Heise Online, 23 de março, 2015, http://www.heise.de/newsticker/meldung/NSA-Skandal-UN-Sonderberichterstatter-fuer-Datenschutz-in-der-digitalen-Welt-angestrebt-2582480.html.

Existem vários exemplos de como houve esforços do governo para implementar a política de encriptação. Eles variam de ações informais a leis e regulamentações.

Lei da Segurança de TI

A Lei de Segurança de TI (*Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme*), que entrou em vigor em julho de 2015, é a consequência da Estratégia de Segurança Cibernética que foi decidida em 2011. Essa lei obriga as transportadoras de infraestruturas particularmente críticas, por exemplo, no setor das telecomunicações, a fornecerem segurança de rede adequada por meio de padrões mínimos e requisitos de notificação de incidentes de segurança de TI.[116]

A lei 'De-Mail'

Um outro exemplo de uma lei que lida explicitamente com técnicas de encriptação é a assim chamada lei 'De-Mail' (*De-Mail Gesetz*), aparentemente indicada após o domínio "*.de"* para a Alemanha. O objetivo legislativo desta lei era estabelecer uma nova funcionalidade de comunicação eletrônica com maior confiança e confiabilidade por meio de técnicas de assinatura e encriptação. Especificamente, a lei também constitui e regula uma nova forma de comunicação pela Internet para entidades privadas.[117] Os serviços de envio De-Mail exigem um credenciamento para a sua prestação de serviços e são supervisionados pelas autoridades (§§ 17-21 da lei De-Mail). A funcionalidade do De-Mail não foi bem-sucedida em relação ao uso, em parte por causa de sua incompatibilidade com o e-mail convencional. Foi criticada também por oferecer segurança abaixo do ideal, uma vez que não implementa encriptação de ponta-a-ponta.[118]

Regulamentações específicas do setor sobre encriptação e segurança da informação

Existem também várias regras específicas do setor para encriptação e segurança da informação na Alemanha. Neste sentido, por exemplo, a Lei das Telecomunicações (TKG) contém padrões para telecomunicações e a Lei da Energia (EnWG) para o setor de energia. Mas em nível europeu, a Diretiva da Rede e de Segurança da Informação (NIS) obrigará os Fornecedores de Serviços Essenciais e Serviços Digitais a serem mais seguros no futuro.[119] Na expectativa de que isso ocorra, a Lei do Escritório Federal de Segurança da Informação (BSIG) já foi atualizada em nível nacional. A lei estabelece obrigações comuns para "infraestrutura crítica" (ver escopo no § 8 c BSIG).

Recomendações e avisos pedagógicos de mídia

116 Detailed presentation at Philipp Roos MMR. Das IT-Sicherheitsgesetz, MMR 2015, p. 636.
117 Com relação à situação atual e à história, ver Alexander Roßnagel. Das De-Mail-Gesetz. NJW 2011, pp. 1473 e seguintes.
118 Cf. Andreas Voßhoff e Peter Büttgen. Verschlüsselung tut Not. ZRP 2014, p. 234.
119 Ver https://ec.europa.eu/digital-agenda/en/news/network-and-information-security-nis-directive.

A segurança na Internet, incluindo informações sobre encriptação, faz parte da educação do público em geral por meio de avisos e recomendações pedagógicas na mídia, oferecidas por instituições governamentais. Assim, o Gabinete Federal para a Segurança da Informação (BSI) e as autoridades de comunicação social do Estado, por exemplo, orientam sobre o uso sensato das mídias sociais e alertam sobre as armadilhas de *phishing*, ou seja, tentativas de enganar os usuários da Internet para que forneçam suas credenciais por meio de mensagens de e-mail falsas. A autoridade estadual de mídia do Saarland, por exemplo, oferece um seminário para encriptar dados com segurança.[120]

O direito fundamental alemão à integridade dos sistemas de TI

No que diz respeito à base constitucional, a decisão do Tribunal Constitucional alemão de 2008 sobre pesquisas online[121] e sua jurisprudência sobre a autodeterminação informacional podem contribuir com informações valiosas para o tratamento legal internacional de técnicas de encriptação. A base para a decisão foi uma norma de autorização de um serviço de inteligência (*Verfassungsschutz Nordrhein-Westphalen*), que permitia o acesso secreto aos sistemas de tecnologia da informação. A norma consistia em dois elementos, permitindo o monitoramento secreto e outras divulgações da Internet (Alt. 1), bem como o acesso secreto aos sistemas de tecnologia da informação (Alt. 2). Analisando cuidadosamente essas disposições à luz da Constituição alemã, o tribunal tomou isso como uma oportunidade para estabelecer padrões elevados em relação à infiltração e manipulação que chegaram muito além dos fatos do caso em questão.

O tribunal criou, especificamente, uma nova dimensão para o direito geral de privacidade: o *direito à proteção da confidencialidade e à integridade dos sistemas de tecnologia da informação* (o chamado "direito básico de TI"). Concluiu que uma interferência nesse direito por infiltração secreta seria apenas admissível no caso de indicações factuais da existência de perigo concreto para um interesse legal predominantemente importante. A infiltração está, em princípio, sujeita a mandado judicial.[122] A dimensão da proteção e a progressão como resultado do avanço tecnológico, que foi perseguida pelo Tribunal, foi amplamente reconhecida e valorizada.[123] Constitui um complemento adequado ao sigilo das telecomunicações, que protege apenas a comunicação em curso, não o sistema em si.

Com o direito básico de TI, o tribunal constitucional reconhece – falando metaforicamente – que partes da personalidade de um indivíduo entram em sistemas de TI e, portanto, a proteção aplicada tem que prosseguir nesse sentido. No campo

120 https://www.lmsaar.de/medienkompetenz/seminare/seminare-nach-themen-2/?mkz-action=details&seminarid=243.

121 BVerfG NJW 2008, 822.

122 BVerfG NJW 2008, 822 (831 et seq.); alguns comentaristas legais criticaram a formulação como implicando um direito fundamental em si, em vez de ser um avanço para o direito existente à autodeterminação informacional, Cf. Martin Eifert. Informationelle Selbstbestimmung im Internet. Das BVerfG und die Online- Durchsuchungen, NVwZ 2008, p. 521; Gabriele Britz, Vertraulichkeit und Integrität informationstechnischer Systeme, DÖV 2008, p. 441.

123 Cf. Thomas Böckenförde. Auf dem Weg zur elektronischen Privatsphäre. JZ 2008, p. 925 et seq.; Gerrit Hornung. Ein neues Grundrecht. CR 2008, p. 299 et seq.; Thomas Stögmüller. Vertraulichkeit und Integrität informationstechnischer Systeme in Unternehmen. CR 2008, p. 435 et seq.

digital, essa ideia está sendo especificada pela decisão do Tribunal Constitucional que já estabeleceu o direito à autodeterminação informacional em 1983.[124]

Vale a pena discutir os detalhes do novo direito com um pouco mais de detalhe. No ambiente digital atual, a autodeterminação protegida requer a possibilidade de autoproteção. Uma maneira importante de obter essa proteção é usando várias técnicas de encriptação no ambiente digital. No entanto, ao se infiltrar no sistema de TI, essa autoproteção é contornada. Isso leva a uma maior dependência por parte do indivíduo em relação a mecanismos e sistemas tecnológicos que estejam fora de seu controle.

O Tribunal Constitucional reconhece isso no que diz respeito ao acesso do serviço de inteligência, que é especificamente direcionado para contornar a tecnologia de encriptação e assim contornar as disposições de autoproteção contra o acesso indesejado a dados do indivíduo-alvo ou de seu provedor de serviços. Considera tal infiltração como uma violação particularmente grave.[125] Em outras palavras, ao indivíduo foi essencialmente concedido o direito de defender-se de forma autônoma contra a infiltração e manipulação de seus dados pessoais. Em resumo, pode-se dizer que, no ambiente digital, o direito à autodeterminação informacional na Alemanha implica o direito de usar encriptação em relação ao seu sistema de TI.

No entanto, outra pergunta que deve ser feita é se a própria Lei Fundamental prevê um "direito à encriptação", que se aplica de forma abrangente. Isso pode ser derivado da combinação de direitos fundamentais individuais. Assim, o sigilo das telecomunicações (Art. 10 I GG) e a inviolabilidade do domicílio (Art. 13 I GG) são também afetados por certos agrupamentos. Através do sigilo tecnologicamente neutro, as telecomunicações atuais são protegidas de abordagens governamentais. Para garantir a confidencialidade dos dados durante a transmissão, parece lógico considerar também o uso de métodos de encriptação protegidos por esse direito.[126]

A redação do novo direito básico de TI traz um elemento de "garantia". Isso ilustra que a decisão vai além da dimensão dos direitos fundamentais como defesa contra a interferência do governo. Segundo o tribunal, o Estado também tem a responsabilidade de proteger a integridade e confiabilidade dos sistemas de tecnologia da informação usados por particulares contra infrações de atores não estatais.

Outro objetivo constitucional é prevenir "*chilling effects*" no exercício das liberdades comunicativas. Este efeito negativo já foi mencionado pelo Tribunal Constitucional em 1983 (Volkszählung).[127] A esse respeito, existe uma relação entre a proteção factual por meio de encriptação e o exercício individual da liberdade, como é o caso, por exemplo, do livre exercício da liberdade de expressão. Somente um exercício destemido das liberdades comunicativas pode ser descrito como verdadeiramente livre segundo o conceito da constituição alemã.

---

124 BVerfGE 65, 1; por exemplo, a fundamentação da proteção de dados na constituição.
125 BVerfG NJW 2008, 822 (830).
126 Gerhards. op cit. p. 126 et seq.
127 BVerfGE 65, 1 (43).

Além disso, uma percepção básica da decisão é que a comunicação moderna depende principalmente de tecnologia. Por conseguinte, uma proteção eficaz dos direitos fundamentais nessa área também requer proteção da infraestrutura de comunicação tecnológica e seu uso.[128] Esta abordagem objetivada e funcional para a proteção dos direitos humanos é fortemente desenvolvida no direito constitucional alemão. A importância do projeto tecnológico voltado para a liberdade de expressão é reconhecida também no debate internacional.[129]

O trabalho alemão sobre privacidade desde o projeto e proteção de dados através da tecnologia

O reconhecimento da impotência individual contra os avanços dinâmicos cada vez mais complexos em sistemas de TI também leva a conceitos de proteção de dados e privacidade por meio de tecnologia e *design*, os quais se aplicam na legislação alemã e ao nível da União Europeia. O objetivo desses princípios é considerar proativamente os interesses de privacidade e proteção de dados nas fases iniciais de sua concepção e do *design* dos sistemas, a fim de evitar um avanço negativo frequentemente irreversível em relação à legislação de segurança de dados.[130] A privacidade desde a fase de *design* (*Privacy by Design*) pode ser um fator de apoio à segurança de dados, à minimização de dados e à capacidade de avanço de sua proteção.

Devido a essa relevância, a proteção de dados por meio da tecnologia e de padrões amigáveis representa um elemento significativo do *Regulamento Geral de Proteção de Dados,* recentemente adotado em nível europeu. São necessárias medidas e procedimentos tecnológicos e organizacionais para garantir que o processamento atenda aos requisitos da promulgação e também da proteção do indivíduo em questão (Art. 23 GDPR). Esta abordagem já é sugerida em nível nacional nos §§ 3, 9 da *Lei Federal de Proteção de Dados* (Bundesdatenschutzgesetz, BDSG), ao passo que o § 3 está centrado na Proteção de Dados do Sistema e no § 9 sobre a Segurança de Dados.[131] Embora a lei nacional alemã possua, desta forma, abordagens inovadoras, elas ainda não estão maduras. Por exemplo, a não observância do § 3 não implica automaticamente na ilegalidade substantiva do processamento de dados, nem em uma sanção.[132] Consequentemente, é difícil avaliar quão efetivas são as abordagens atualmente.

Índia

Embora a lei e a política indiana promovam e exijam a implementação de encriptação forte como medida de segurança, como em bancos, comércio eletrônico e

---

128 Wolfgang Hoffmann-Riem. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. JZ 2008, p. 1009 et seq.

129 Cf. Jack Balkin. Digital Speech and Democratic Culture: a Theory of Freedom of Expression for the Information Society. NYU Law Review 79 (2004).

130 Cf. Voßhoff/Büttgen op. cit. p. 232.

131 Ernestus in Simitis. Bundesdatenschutzgesetz. § 9 retical 1 et seq; Gola/Klug/Körffer in Gola/Schomerus. Bundesdatenschutzgesetz. § 9 retical 1 et seq; Jörg Pohle critica esta opinião predominante em: Das Scheitern von Datenschutz by Design: Eine kurze Geschichte des Versagens. FlfF-Kommunikation 2/15, 41 seq.

132 Schulz op. cit. p. 208.

organizações que lidam com informações pessoais confidenciais, há uma série de limitações na implantação gratuita de encriptação pelos serviços de comunicações eletrônicas. Especificamente, os contratos de licença com serviços regulamentados pela estrutura de telecomunicações contêm restrições que permitem apenas níveis de encriptação de 40 bits (detalhes explicados abaixo). Quando uma encriptação forte é implantada por esses serviços, há uma prática de registro e custódia de chaves de interesse do acesso legal do governo a comunicações de texto simples. Há uma notável incerteza jurídica sobre o escopo legal preciso desses requisitos de licença e em que medida eles poderiam ter efeito legal sobre (o uso ou a implantação de) serviços utilizados pelos usuários finais de serviços cobertos. Essa incerteza jurídica parece ser prejudicial ao desenvolvimento, implantação e uso de encriptação forte na Índia para comunicações:

> negócios avessos ao risco não podem exceder seus níveis de encriptação além de 40 bits; caso contrário, eles podem correr o risco de divulgar a "chave de desencriptação" para o governo da Índia e ter que buscar sua aprovação prévia.[133]

O debate público sobre encriptação foi iniciado recentemente na Índia, depois que o governo publicou uma proposta preliminar com uma série de limitações previstas no uso da encriptação. A política,[134] expedida sob a Seção 84A da Lei de Tecnologia da Informação Indiana (Emenda), 2008[135] teve curta duração, mas ainda há preocupações sobre a falta de garantias de privacidade e de liberdade de expressão esboçadas na proposta.[136] Em resposta aos protestos generalizados, o governo indiano primeiro isentou "produtos de encriptação de uso em massa, que atualmente estão sendo usados em aplicativos da Internet, *sites* de mídia social e aplicativos de mídia social, como WhatsApp, Facebook, Twitter etc."[137] Logo em seguida, o governo se absteve da política proposta e ainda não foi publicada uma nova política..

A seção 84A da Lei de Tecnologia da Informação Indiana (Emenda) de 2008 concede poderes ao governo para formular regras sobre modos de encriptação para o meio eletrônico. Prevê que: "O Governo Central pode, para uso seguro do meio eletrônico e para a promoção da governança eletrônica, prescrever os modos ou métodos de encriptação." O texto desta disposição sugere que essa se destina a autorizar o Governo Central a elaborar regras de interesse da segurança na rede, promoção de comércio eletrônico e uso de governo eletrônico. Depreende-se do projeto de política

---

133 Apar Gupta. How many bits are enough? the legality of encryption. Novembro de 2011. http://www.iltb.net/2011/11/how-many-bits-are-enough-the-legality-of-encryption/.

134 Indian Government Draft Policy. Setembro de 2015. Disponível em http://www.scribd.com/doc/282239916/ DRAFT-NATIONAL-ENCRYPTION-POLICY (último acesso: 14 de setembro de 2016).

135 Disponível em http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf (último acesso: 14 de setembro de 2016).

136 Bhairav Acharya. The Short-lived Adventure of India's Encryption Policy. Dezembro de 2015. https://www.ocf. berkeley.edu/~bipla/the-short-lived-adventure-of-indias-encryption-policy/.

137 Nandagopal Rajan. Encryption Policy: WhatsApp, Web services out of draft encryption policy after outcry. Setembro de 2015. http://indianexpress.com/article/technology/tech-news-technology/draft- national-encryption-policy-you-might-need-to-store-whatsapp-messages-for-90-days/. (Último acesso:
14 de setembro de 2016). No Twitter, usuários preocupados se reuniram em torno da *hashtag* #ModiDontReadMyWhatsapp.

que o governo indiano considera o Artigo 84A como fundamentação jurídica para restringir o uso de encriptação forte — em vez de exigi-la ou promovê-la— ou como reconhecimento de que o uso de encriptação na esfera comercial ou privada requer autorização do Governo, sinalizando a existência de uma proibição geral sem permissão.

Comentaristas jurídicos notaram a falta de transparência sobre quais tipos de uso e implantação de encriptação são permitidos e exigidos pela lei indiana, especialmente no campo de serviços de comunicações eletrônicas.[138] Um dos motivos da insegurança jurídica advém da área do Direito das telecomunicações. Uma ampla estipulação do poder exclusivo do governo sobre o estabelecimento, manutenção e trabalho dos telégrafos é concedida no *Indian Telegraph Act*, 1885 (e emendas), que fornece o principal quadro regulamentar para os serviços de comunicações na Índia (Seção 4 (1)). A seção 3 (1) da Lei, define o termo "telégrafo" amplamente para incluir:

> … qualquer aparelho, instrumento, material ou aparato usado ou capaz de ser usado para transmissão ou recepção de sinais, sinalizações, escrita, imagens e sons ou inteligência de qualquer natureza por fio, imagens, ou outras emissões eletromagnéticas, ondas de rádio ou ondas hertzianas, galvânicas, elétricas ou magnéticas.[139]

Assim, o Governo Central da Índia tem, teoricamente, um amplo monopólio sobre comunicações eletrônicas que incluem o privilégio de fornecer serviços de telecomunicações e Internet na Índia. Essa disposição continua a ser aplicável à prestação de serviços abrangidos pelos regulamentos de telecomunicações, não obstante a liberalização das telecomunicações desde 1999.[140] O Governo da Índia permitiu que *players* privados prestassem serviços relevantes de telecomunicações e Internet, celebrando acordos mútuos de licenciamento. Esses contratos de licença preveem cláusulas sobre o uso de encriptação.[141] Especificamente, o Contrato de Licença para a Prestação de Serviços da Internet (Cláusula 2.1 (vii)) declara que:

> (vii) O Licenciado deverá garantir que a Encriptação em Massa não seja implantada pelos ISPs. Além disso, indivíduos/grupos/organizações podem usar encriptação de até 40 bits nos algoritmos de chave simétrica ou seu equivalente em outros algoritmos sem obter permissão do Licenciante. No entanto, se equipamentos de encriptação superior a esse limite forem instalados, pessoas físicas/grupos/organizações devem obter permissão prévia por escrito do Licenciante e depositar a chave de desencriptação, dividida em duas partes, juntamente com o Licenciante.

Esses níveis predeterminados de encriptação geralmente permitidos (simétricos) (40 bits) podem ser considerados inseguros. O nível de 40 bits, em particular,

---

138 Apar Gupta. How many bits are enough? the legality of encryption. Novembro de 2011. http://www.iltb.net/2011/11/how-many-bits-are-enough-the-legality-of-encryption/.

139 India Telecom Laws and Regulations Handbook, 2013. Volume 1, p. 179.

140 Cf. Indian National Telecom Policy of 1999 http://www.dot.gov.in/telecom-polices/new-telecom-política-1999; e versão mais recente de 2012. http://www.dot.gov.in/sites/default/files/NTP-06.06.2012- final.pdf.

141 Apar Gupta. op. cit.

corresponde ao nível de encriptação permitido anteriormente nos EUA para os controles de exportação. Recentemente, uma vulnerabilidade de segurança foi constatada na implementação de comunicações seguras com *sites*. Esta vulnerabilidade explorou a possibilidade de forçar conexões entre usuários e *sites* para degradar a encriptação para esses níveis de proteção de exportação anteriores. Isso demonstra como o impacto negativo das restrições à segurança na prática pode durar muito mais do que o tempo de vida útil legal das mesmas.

Além disso, a linguagem nos contratos de licença sobre o uso de encriptação mais forte reflete a prática da custódia de chaves na Índia. A custódia de chaves foi ilustrada pelo caso amplamente discutido sobre as operações da Blackberry na Índia, analisada a seguir.[142] O Contrato de Licença do Serviço de Telefonia Celular Móvel prevê restrições semelhantes sobre o uso de encriptação e requer inspeção e aprovação de dispositivos de usuários finais que implementam encriptação forte.[143] Embora essas disposições de licença sinalizem um ambiente mais restritivo, o setor privado implementou versões robustas de encriptação que excedem o nível de 40 bits.

As propostas preliminares de política de encriptação com base na Seção 84^{A}, publicadas pelo governo indiano, seguem um processo consultivo que ocorreu após a adoção desta disposição em 2008. Em particular, em 2009, o Conselho de Segurança de Dados da Índia emitiu recomendações para a política de encriptação.[144] Considerações sobre direitos humanos foram relativamente pouco desenvolvidas nesta recomendação, que discutiu as necessidades das agências governamentais de direito indiano em obter acesso a algum detalhe de texto não encriptado. A recomendação afirma o seguinte sobre os interesses em questão:

> A política de encriptação exige a consideração de vários problemas técnicos, questões de segurança nacional, privacidade de negócios, e pressões competitivas internacionais para o crescimento das aplicações de comércio eletrônico e de governança eletrônica. O crescimento econômico contínuo das indústrias e empresas indianas em uma economia cada vez mais global requer disponibilidade de encriptação para todos os usuários legítimos, que incluem funcionários e parceiros de negócios do setor corporativo.

Isso sinaliza fortes considerações nas políticas de competitividade econômica indiana internacionalmente. Especificamente, o Conselho de Segurança de Dados observa que "empresas estrangeiras tendem a restringir a terceirização para a Índia se textos simples forem solicitados por órgãos de aplicação da lei sem o devido processo e/ou ordens judiciais".[145] A recomendação propõe promover e liberalizar a encriptação, não adotar requisitos de registro e estipula a maneira pela qual o acesso a textos simples pela aplicação da lei pode ser geralmente assegurada, ao mesmo tempo respeitando as garantias do devido processo legal.

---

142 Cf. Paul Taylor. Security that makes spies feel insecure. *Financial Times*. 2 de agosto de 2010, http://www. ft.com/intl/cms/s/0/7ad48c10-9e5d-11df-a5a4-00144feab49a.html#axzz3R5nCIW6I.

143 Apar Gupta. op cit.

144 Ver Recommendations for Encryption Policy u/s 84A of the IT (Amendment) Act, 2008.

145 Recommendations for Encryption Policy u/s 84A of the IT (Amendment) Act, 2008, pág. 11.

Um exemplo de custódia de chaves e práticas de licenciamento no sistema legal indiano, e da maneira como elas interagem com empresas de serviços de comunicação operando internacionalmente, é o caso da Blackberry, que foi discutido na mídia internacional.[146] O governo indiano exigiu que a BlackBerry permitisse o monitoramento de seus e-mails e SMS.[147] Para dar conta das solicitações legais de acesso das autoridades indianas, a BlackBerry criou um escritório doméstico em Mumbai. Embora os detalhes não sejam conhecidos, parece que, nesse caso, as chaves foram mantidas em custódia pela própria Blackberry.

Na área de serviços financeiros e comércio, existem regulamentações específicas sobre níveis exigidos de encriptação por partes interessadas relevantes. De acordo com as diretrizes do *Reserve Bank of India*, para todas as transações bancárias é previsto um mínimo de encriptação SSL de 128 bits (Camada de Soquete Seguro). O Conselho de Valores Mobiliários da Índia (SEBI) prescreve uma encriptação de 64 bits/128 bits para segurança de rede padrão e exige o uso da respectiva tecnologia para segurança, confiabilidade e confidencialidade dos dados.[148] Nas Normas de Tecnologia da Informação (Autoridades de Certificação) de 2000, o Governo Central Indiano estipula uma estrutura de métodos criptográficos para assinaturas digitais e padrões criptográficos relacionados de chave pública.[149] Há também Normas de Tecnologia da Informação, de 2011, (práticas e procedimentos de segurança razoáveis e dados ou informações pessoais sensíveis), baseadas no Artigo 43A da Lei de Informática, que exigem a implementação de práticas razoáveis de proteção e segurança de dados no que diz respeito a informações sensíveis por parte de atores comerciais, inclusive para dados biométricos, informações médicas, orientação sexual e senhas.[150]

Na última década, houve certo apoio internacional para a Índia se unir ao Acordo Wassenaar sobre Controles de Exportação de mercadorias de uso duplo.[151] A regulamentação indiana sobre comércio exterior prevê restrições à exportação de "Tecnologia da informação, incluindo segurança da informação" e "equipamento de segurança de processamento de dados, equipamento de segurança de dados de linha de transmissão e sinalização, usando processos de *ciphering*", [152] que é a linguagem idêntica à usada no Acordo de Wassenaar, na "*Munitions List*".[153] Não há

146 Para discutir o assunto, ver também *Citizen Lab (Munk School of Global Affairs*, Universidade de Toronto) e Collin Anderson t. The Need for Democratization of Digital Security Solutions to Ensure the Right to Freedom of Expression.10 de fevereiro de 2015. http://www.ohchr.org/Documents/Issues/Opinion/Communications/ CitizenLab.pdf.

147 A. Parvathy, Ravi Shankar Choudhary and Vrijendra Singh. Legal Issues Involving Cryptography in India. Abril de 2013 *International Journal of Computer Application*, edição 3, volume 2, http://rspublication.com/ijca/april13/6.pdf. Ver também Citizen Lab e Collin Anderson 2015.

148 Section 3(a) and referenced DOT Policy,http://www.nseindia.com/invest/resources/download/sebi_ circ_27082010.pdf.

149 Information Technology (Certifying Authorities) Rules of 2000, http://cca.gov.in/cca/sites/default/files/files/ rules.pdf (último acesso: 14 de setembro de 2016).

150 Ministério das Comunicações e Tecnologia da Informação, Notificação, Nova Deli, 11 de abril de 2011, http:// www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf (último acesso: 14 de setembro de 2016).

151 O Acordo Wassenaar sobre Controles de Exportação para Armas Convencionais e Bens e Tecnologias de Dupla Utilização. Ver http://www.nti.org/treaties-and-regimes/wassenaar-arrangement/ no apoio de membros da Índia.

152 Ministério do Comércio e Indústria, Notificação No. 14 (RE-05)/2004-2009, Nova Deli; 15 de julho de 2005, linkhttp://www.vertic.org/media/National%20Legislation/India/IN_Amendment_of_ITC_HS_Export_and_ Import_Classification_2005.pdf (último acesso: 14 de setembro de 2016).

153 http://www.wassenaar.org/wp-content/uploads/2015/06/WA-LIST-13-1.pdf.

dados sobre interpretação e aplicação dessas regras na prática.

Brasil

Após as revelações de Snowden, o Brasil esteve na vanguarda de uma coalizão global de promoção de direito à privacidade na ONU e condenando a vigilância em massa dos EUA. Em eventos recentes, o Brasil demonstrou diversos objetivos em relação ao uso e implementação de encriptação. Por um lado, o país é líder no fornecimento de uma estrutura jurídica de regras para a Internet. Por outro lado, foram tomadas várias medidas que podem restringir a disseminação da tecnologia de encriptação.

Atualmente, não há controles de exportação/importação na tecnologia de encriptação no Brasil, relacionados a software ou hardware. Tampouco existem controles quanto ao uso de tecnologia criptográfica. Em 2015, em um processo aberto a comentários e discussões do público, o legislador brasileiro elaborou um novo projeto de lei de proteção de dados,[154] que foi encaminhado ao Congresso Nacional do Brasil em 13 de maio de 2016 e passou a existir como Projeto de Lei 5.276 de 2016. Este regula e protege dados pessoais e privacidade, incluindo práticas *online*, bem como disposições para métodos mais seguros, como encriptação no tratamento de dados pessoais. A lei proposta aborda ainda questões de segurança e o dever das empresas de relatar quaisquer ataques e violações de segurança. No artigo 44.º, inciso III, afirma:

> *o controlador deve comunicar imediatamente qualquer incidente de segurança que possa causar danos aos titulares dos dados ao organismo competente.*
>
> *A notificação deve incluir, pelo menos: [...]*
>
> *III – especificação das medidas de segurança utilizadas para proteção dos dados, inclusive eventuais procedimentos de encriptação;*[155]

Além disso, nenhuma disposição sobre encriptação consta do referido projeto de lei.

Na ocasião da presente redação, a crise do governo e os protestos em todo o país resultantes de vários casos de corrupção evidenciados, abrangendo não apenas partes do governo, mas também militares e o Judiciário[156], despertaram novos temores na sociedade civil quanto ao enfraquecimento do Estado de direito. Resta saber se estes desenvolvimentos provarão exercer um impacto mais intenso na política de informação e comunicação, incluindo a encriptação.

---

154 Disponível em http://pensando.mj.gov.br/dadospessoais/ (último acesso: 14 de setembro de 2016).

155 Projeto de Lei, sobre o tratamento de dados pessoais para proteger a personalidade e dignidade das pessoas físicas. Link http://pensando.mj.gov.br/dadospessoais/wp-content/uploads/sites/3/2015/02/Brazil_pdp_ bill_Eng1.pdf (último acesso: 14 de setembro de 2016).

156 Glenn Greenwald, Andrew Fishman e David Miranda, 'New Political Earthquake in Brazil: Is It Now Time for Media Outlets to Call This a "Coup"?' The Intercept, 23 de maio de 2016, https://theintercept.com/2016/05/23/ new-political-earthquake-in-brazil-is-it-now-time-for-media-outlets-to-call-this-a-coup/.

O Marco Civil

Com o Marco Civil da Internet, o Brasil foi um dos primeiros países a introduzir uma lei que visa combinar todas as regras da Internet em um único pacote. Com aprovação do Senado e sanção pela então presidente Dilma Rousseff, a lei entrou em vigor em abril de 2014.[157] Embora princípios como liberdade de expressão e privacidade já estejam protegidos pela constituição brasileira, a nova lei especifica como esses princípios se aplicam ao ambiente *online*. Além disso, introduz e estipula novos princípios, como a neutralidade da rede:

> *Art. 9: O responsável pela transmissão, comutação ou roteamento tem o dever de tratar, de forma isonômica, quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.*

No Art. 7, X, o Marco Civil esclarece que a proteção de dados pessoais é importante do ponto de vista da privacidade e exige a eliminação de tais dados por solicitação do usuário ou após o término do relacionamento entre as partes.

> *Art. 7: O acesso à Internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:*
>
> *(X) exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de Internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;*

Embora não haja disposições textuais quanto ao direito à encriptação, o Marco Civil prevê a proteção do sigilo da comunicação do usuário em várias disposições, conforme o Art. 7 II, III e art. 11. Não se compreende claramente, no entanto, se isso inclui encriptação.

> *Art. 7: O acesso à Internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:*
>
> (II) inviolabilidade e sigilo do fluxo de suas comunicações pela Internet, salvo por ordem judicial, na forma da lei;
>
> (III) inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

e

> *"Art. 11: Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de Internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo*

---

157 The Brazilian Civil Rights Framework for the Internet, disponível em http://direitorio.fgv.br/noticia/the-brazilian-civil-rights-framework-for-the-Internet.

das comunicações privadas e dos registros."

Tecnologia de encriptação no setor privado brasileiro

Em comparação com alguns outros países, a encriptação ainda desempenha apenas um papel menor para as empresas brasileiras. Portanto, o legislador busca introduzir medidas de encriptação e privacidade, conforme visto acima.

Entretanto, muitas empresas apresentam um perfil de segurança frágil. Em média, as organizações brasileiras dedicam uma porcentagem menor de seus orçamentos de TI a tecnologias de encriptação do que outros países.[158] Parece, portanto, que o maior desafio no Brasil em relação à encriptação consiste na implementação dos métodos e padrões existentes por organizações relevantes, inclusive no governo e na indústria.

Um grande incentivo para as empresas usarem criptografia, imediatamente após o cumprimento dos regulamentos, é proteger a marca ou evitar danos à reputação por violação de dados. No entanto, um relatório recente mostrou que surpreendentes 46% das empresas entrevistadas no Brasil admitiram ter apenas um plano ou estratégia de encriptação limitada ou inexistente.[159] Mais da metade delas declararam que não possuem um líder funcional que seja responsável por determinar o uso da encriptação. Em suma, o gerenciamento de identidades e acessos, seguido pela constatação de dados em risco, são as duas maiores prioridades de proteção de dados.[160]

Governo eletrônico e participação

Em relação às formas modernas de interação entre os cidadãos e o governo, o Brasil possui um modelo bem estabelecido de governo eletrônico: Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).[161] Foi introduzido em agosto de 2001, juntamente com a Medida Provisória 2.200-2. A lei em si consiste principalmente na segurança de infraestrutura relevante. No Artigo 10, entretanto, estabelece a validade legal dos certificados ICP-Brasil baseados em assinaturas digitais. O certificado em si é gerado e assinado por um terceiro confiável, ou seja, uma autoridade de certificação. Este contém os dados do titular, como nome e número de registro civil e a assinatura da autoridade de certificação. Desde 2010, os certificados ICP-Brasil podem ser parcialmente integrados em identidades brasileiras, podendo então ser usados para vários serviços, como serviço de receita fiscal, serviços judiciais ou serviços

158 cf. Thales 2016. Global Encryption Trends Study: Brazil, https://www.thales-esecurity.com/knowledge-base/ analyst-reports/global-encryption-trends-study.

159 Estudo Global sobre Tendências de Encriptação da Thales 2016: Brasil, https://www.thales-esecurity.com/knowledge-base/ analyst-reports/global-encryption-trends-study.

160 Embora essa provavelmente não tenha sido a intenção, alguns efeitos do Marco Civil já estão sendo sentidos de forma negativa. As disposições exigindo neutralidade da rede, que deveriam proteger a liberdade na Internet, se revelaram contraproducentes, quando se trata de acesso à informação. Como proíbe empresas privadas de oferecerem acesso livre e aberto à Internet, aplicativos de smartphones que oferecem acesso gratuito a determinadas páginas são vistos como contrários ao código. Um exemplo notável é o "Projeto Wikipedia Zero", com o objetivo de promover o acesso à informação pela Wikipedia.org em dispositivos móveis gratuitos, é proibido pelos princípios de neutralidade da rede do Marco Civil.

161 Para mais informações, consulte http://www.iti.gov.br/icp-brasil.

relacionados a bancos. Na prática, o certificado digital ICP-Brasil atua como uma identidade virtual que permite a identificação segura e única do autor de uma mensagem ou transação efetuada em meios eletrônicos, como a Web. No entanto, o nível de integração ainda é insuficiente.

Bloqueio do WhatsApp

Em eventos recentes, alguns tribunais brasileiros se opuseram à encriptação em serviços de mensagens privadas, ordenando repetidamente o bloqueio do serviço de mensagens WhatsApp.[162] Desde que mudou para uma encriptação completa de ponta-a-ponta, o serviço foi bloqueado periodicamente como resultado de uma ordem judicial na tentativa de fazer com que a empresa obedeça às demandas por informações. Consequentemente, outros serviços de mensagens encriptados, como o Telegram ou o Viber, registraram saltos em número de inscrições. O Telegram afirmou ter ganho mais de um milhão de novos usuários dentro de dias, após o bloqueio se tornar público (o serviço tem mais de 100 milhões de usuários ativos, no total).[163] É evidente que existe uma demanda generalizada por comunicações encriptadas entre os brasileiros. Essa tendência parece ser reforçada pelas tentativas de se impedir o uso de serviços encriptados.

A Região Africana

Como resultado da opção neste estudo para não discutir a política de encriptação em um país específico na região africana, as evidências fornecidas abaixo referem-se a diversos países do continente africano. A região africana é diversificada quando se trata de quadros jurídicos nacionais existentes em nível nacional. Para fornecer algumas evidências sobre a política de encriptação e seu contexto, este estudo de caso divide a região africana em diferentes grupos de países, depois de fornecer algumas informações gerais sobre o continente africano, essas sub-regiões africanas refletem comunidades econômicas regionais, como a CEDEAO (Comunidade Econômica dos Estados da África Ocidental), EAC (Comunidade da África Oriental), COMESA (Mercado Comum da África Oriental e Austral), ECCAS (Comunidade Econômica dos Estados da África Central).

A União Africana é a organização intergovernamental africana regional (incluindo o norte da África) que forneceu algumas orientações legais e normativas específicas para o continente africano. A Carta Africana (Banjul) sobre os Direitos Humanos e dos Povos foi adotada no contexto da União Africana em 1981.[164] A supervisão e interpretação da Carta de Banjul é de responsabilidade da Comissão Africana dos Direitos Humanos e dos Povos. Um Protocolo à Carta, que estabelece o Tribunal Africano dos Direitos Humanos e dos Povos, foi adotado em 1998 e entrou em vigor em 2005. Apenas sete Estados-membros da União Africana reconheceram o direito

---

162 Stephanie Mlot, Brazil Bans WhatsApp (Again) Over Encryption, pcmag, 3 de maio de 2016, http://www.pcmag. com/news/344200/brazil-bans-whatsapp-again-over-encryption.

163 Telegram Messenger (@telegram), Twitter, 2 de maio de 2016, https://twitter.com/telegram/status/727200237308227585.

164 Carta Africana (Banjul) sobre os Direitos Humanos e dos Povos, Adotada em 27 de junho de 1981, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), entrou em vigor em 21 de outubro de 1986.

de instaurar processos judiciais, enquanto em fevereiro de 2016, 30 dos 54 Estados-membros ratificaram o protocolo. Na área da política de informação, a União Africana adotou a Convenção da União Africana sobre Segurança Cibernética e Proteção de Dados Pessoais.[165] As disposições sobre proteção de dados pessoais na presente Convenção seguem em geral o modelo europeu para a proteção da privacidade dos dados e contém várias disposições sobre a segurança do processamento de dados pessoais. Uma iniciativa da sociedade civil adotou uma Declaração Africana específica sobre Direitos e Liberdades na Internet "para ajudar a adequar as abordagens sobre criação de políticas e governança da Internet em todo o continente".[166]

O impacto das leis-modelo, promovidas por organizações governamentais internacionais, dentre elas, a *Commonwealth* e a *le Francophonie*, bem como organismos de normatização internacional de telecomunicações, poderia influenciar significativamente as questões políticas específicas discutidas neste relatório, mas uma análise dessa influência vai além do escopo deste estudo.

A porcentagem de usuários da Internet na África é ainda muito inferior à média mundial, o que explica a (relativa) falta de legislação a respeito. Enquanto o resto do mundo constata uma penetração de quase 50% dos usuários da Internet de toda a população a partir de 2015, o continente africano permanece em 28,6%.[167] Espera-se que a revolução móvel em andamento seja capaz de alterar esses números; contudo, é provável que o acesso à Internet continue a ser o principal desafio na área de políticas para a Internet.

Norte da África [168]

Mesmo com as transformações iniciadas no ano de 2011, diferentes países da região Norte-Africana não constataram um aumento significativo das ações judiciais relativas a suspensão da encriptação. No entanto, embora a legislação muitas vezes remonte a antes das transformações, a imposição tornou-se mais rigorosa desde então. Nenhuma diferença na posição em relação à criptografia pode ser vista entre os países que tiveram revoluções bem-sucedidas e passaram por mudanças de regime, como a Tunísia, e aqueles que não o fizeram.

A Tunísia tem diversas leis que limitam o anonimato *online*. Os artigos 9º e 87º do Código das Telecomunicações de 2001 proíbem a utilização de encriptação e preveem sanções de até cinco anos de prisão pela venda e uso não autorizado de tais técnicas.[169] Embora essas leis tenham sido promulgadas, ainda com base na

165 Convenção da União Africana sobre Segurança Cibernética e Proteção de Dados Pessoais, adotada em 27 de junho de 2014. A Convenção foi assinada por 8 dos Estados Membros.

166 Ver African Declaration on Internet Rights and Freedoms, disponível em http://africanInternetrights.org/ (último acesso 14 de setembro de 2016).

167 Internet World Stats, http://www.Internetworldstats.com/stats1.htm (último acesso 14 de setembro de 2016).

168 O projeto SMEX sobre Legislação Árabe e Ordens que afetam os Direitos Digitais, disponibiliza algumas referências às leis pertinentes na região, embora não especificamente sobre a questão da encriptação. Consulte https://smex.silk.co/ (último acesso em 14 de setembro de 2016).

169 Lei n ° 1-2001 de 15 de janeiro de 2001, relativa à promulgação do código de telecomunicações (Tunísia), disponível emhttp://www.wipo.int/wipolex/en/text.jsp?file_id=204160 (acessado pela última vez: 14 de setembro de 2016).

regra do governo anterior, até agora não houve esforços bem-sucedidos para tornar as disposições relevantes mais permissivas. Tampouco, não houve relatos recentes sobre o cumprimento dessas leis. Ainda assim, a confirmação de sua existência pode ser interpretada como a hesitação dos países de seguir uma abordagem mais permissiva em relação ao uso de técnicas criptográficas no ambiente de comunicação e mídia.

Na Argélia, os usuários precisam de autorização legal para o uso da tecnologia criptográfica da relevante autoridade de telecomunicações ARPT (Autorité de Régulation de la Poste et des Télécommunications) desde 2012.[170] No Egito, o Artigo 64 da Lei de Regulamentação de Telecomunicações de 2003 declara que o uso de dispositivos de encriptação é proibido sem o consentimento por escrito do NTRA, das autoridades militares e de segurança nacional.[171] Embora decretada durante a era anterior, a lei ainda está em vigor. Além disso, os usuários de cybercafés precisam obter um PIN para acessar a Internet. Portanto, eles precisam se registrar com seu nome, endereço de e-mail e número de celular. Todas essas informações *online* podem ser acessadas pelos escritórios da Presidência, Segurança, Inteligência, e da Autoridade de Controle Administrativo sem o prévio consentimento do tribunal, se a segurança nacional estiver em pauta.

O Egito foi relatado como usuário de um software chamado "Sistema de Controle Remoto", que pode capturar dados no computador de destino, monitorar comunicações encriptadas na Internet, gravar chamadas, e-mails, mensagens e senhas do Skype digitadas em um navegador e ligar remotamente a Webcam e o microfone de um dispositivo.[172] O Egito supostamente bloqueou o serviço "*free basics*" do Facebook no final de 2015, após não conseguir obter a cooperação do Facebook em questões relacionadas ao acesso aos dados de seus usuários.[173]

No Marrocos, a importação e exportação de tecnologia criptográfica, seja software ou hardware, requer uma licença do governo. A lei pertinente nº 53-05 (Lei nº 53-05 *relative à l'échange électronique de données juridiques*) entrou em vigor em dezembro de 2007. O Art. 13 declara:

> *A fim de impedir a sua utilização para fins ilegais e proteger os interesses da defesa nacional ou da segurança externa e interna do Estado, a importação, exportação, fornecimento, operação ou o uso de meios para serviços criptográficos está sujeito a: a) uma declaração prévia, ao utilizar este serviço*

---

170 Decisão n.o 17, de 11 de junho de 2012, http://www.arpt.dz/fr/doc/reg/dec/2012/DEC_N17_11_06_2012.pdf (último acesso: 14 de setembro de 2016).

171 Lei de Regulamentação das Telecomunicações do Egito (Tradução), disponível emhttp://hrlibrary.umn.edu/research/ Egypt/Egypt%20Telecommunication%20Regulation%20Law.pdf (último acesso: 14 de setembro de 2016).

172 Consulte o Citizen Lab, Mapping Hacking Team's "Untraceable" Spyware, a Monk School of Global Affairs, 17 de fevereiro de 2014, https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/ (último acesso: 14 de setembro de 2016). Ver também Emir Nader, Egypt's purchase of hacking software documented in new leaks, Daily News Egypt, 6 de julho de 2015,http://www.dailynewsegypt.com/2015/07/06/egypts-purchase- of-hacking-software-documented-in-new-leaks/ (último acesso: 14 de setembro de 2016).

173 Ver Yasmeen Abutaleb e Joseph Menn, Exclusive: Egypt blocked Facebook Internet service over surveillance – sources, Reuters, 1 de abril de 2016,http://www.reuters.com/article/us-facebook-egypt-idUSKCN0WY3JZ (último acesso 14 de setembro de 2016).

tem o único propósito de autenticar a transmissão ou garantir a integridade dos dados transmitidos eletronicamente; b) uma aprovação prévia da administração, quando se tratar de uma finalidade diferente da especificada no parágrafo a) supra.

Os artigos 32, 33 e 34 estipulam as penalidades para as violações do Artigo 13, com pena de prisão de um ano e multas de 100.000 MAD ou cerca de 10.000 dólares norte-americanos. Desde fevereiro de 2015, a autoridade relevante para a aprovação e o monitoramento da tecnologia de encriptação não é mais uma agência civil, mas um órgão militar, o DGSSI (*Direction General de la Securité des Systèmes d'Information*).[174]

Por fim, uma tendência que limita a encriptação em favor da vigilância do governo é perceptível nos Estados do norte da África. O uso da tecnologia de encriptação é proibido ou severamente restrito.

África Oriental

Não parece haver qualquer norma específica em vigor nos países da região da África Oriental que restrinjam o uso da tecnologia de encriptação. No entanto, os poderes de vigilância do Estado parecem estar se expandindo. Como em outros países africanos, a principal razão é a prevenção de ataques terroristas. O Quênia, com sua proximidade com a Somália, citou essa ameaça por adotar ações restritivas. Recentemente, o país acelerou a aprovação da Lei de Informática e Crime Cibernético, adotada no final de 2016.[175] O projeto de lei, que tem por base a Convenção Europeia sobre Crimes Cibernéticos, prevê disposições específicas sobre encriptação, no contexto da aplicação da lei, o acesso aos dados em relação às investigações. Essas disposições permitem uma ordem para desencriptar informações e comunicações armazenadas, em provedores de serviços com essa capacidade para desencriptar. Na Etiópia, conhecida por leis rigorosas em relação a atividades online, vários blogueiros acusados de terrorismo também foram acusados de encriptar suas comunicações.[176]

Em Uganda, várias leis e políticas de TIC foram aprovadas nos últimos três anos, mas nenhuma delas trata da encriptação. Em 2016, após as eleições presidenciais, o governo ugandense fechou redes sociais, como Twitter, Facebook e WhatsApp.[177]

---

174 Bulletin officiel n° 6332 du 15 rabii II 1436 (5 de fevereiro de 2015), disponível em http://adala.justice.gov.ma/ production/html/Fr/liens/..%5C188896.htm (último acesso: 14 de setembro de 2016).

175 Ver MyGov, Computer and cybercrime law to be in place before end year, 29 de junho de 2016, http://www. mygov.go.ke/?p=10848 (último acesso: 14 de setembro de 2016).

176 Ver Endalk Chala, What You Need to Know About Ethiopia v. Zone9 Bloggers: Veredicto previsto para 20 de julho, *Global Voices Advox*, 17 de julho de 2015, https://advox.globalvoices.org/2015/07/17/what-you-need-to-know- about-ethiopia-v-zone9-bloggers-verdict-expected-july-20/ (último acesso em 14 de setembro de 2016). Ver também *Freedom House, Freedom on the Net* 2015: Etiópia, https://freedomhouse.org/sites/default/files/ resources / FOTN% 202015_Ethiopia.pdf (último acesso: 14 de setembro de 2016).

177 Ver BBC News, Uganda Election: Facebook and Whatsapp blocked, 18 de fevereiro de 2016, http://www.bbc. com.br/notícias/world-africa-35601220 (último acesso: 14 de setembro de 2016). Ver também Nshira Turkson, A SocialMedia Shutdown in Uganda's Presidential Elections The Atlantic, 18 de fevereiro de 2016, http://www.theatlantic. com/international/archive/2016/02/uganda-election-social-

Nenhuma diferença parece ter sido efetuada entre serviços usando encriptação de ponta-a-ponta e outros. Como muitos usuários optaram pelo uso de serviços VPN para contornar restrições, eles foram capazes de limitar a extensão em que foram afetados por essas ações restritivas.

África Ocidental

A Nigéria, o país mais populoso do continente, tem o maior número de usuários da Internet em toda a África: 51% da sua população.[178] Em países como Gana e Costa do Marfim, a porcentagem populacional “online" é de apenas 20%[179]. Embora os países da África Ocidental não pareçam limitar a importação ou exportação de tecnologia de encriptação, nem o seu uso, a maioria das empresas nacionais e estrangeiras ainda conta com o uso de VPNs para sua comunicação.

Gana introduziu recentemente um projeto de lei visando interceptar comunicações eletrônicas e postais dos cidadãos para ajudar ostensivamente na prevenção do crime. A Seção 4(3) do projeto de lei proposto concede a permissão do governo para interceptar a comunicação de qualquer pessoa somente por meio de solicitação verbal de um agente público.[180] Embora outras disposições estipulem a necessidade de uma decisão judicial, a Seção 4(3) substitui todas elas, basicamente concedendo ao governo poder ilimitado para monitorar a comunicação sem ordem judicial. Considerando esses assuntos, o Comitê de Direitos Humanos da ONU solicitou que Gana fornecesse garantias legais para evitar o abuso da lei.[181]

Recentemente, a Comissão de Comunicações da Nigéria elaborou um projeto de lei relativo à interceptação legal das regulamentações de comunicação.[182] Se aprovada, a lei permitirá a interceptação de toda comunicação sem supervisão judicial ou ordem judicial e obrigará as empresas de telefonia móvel a armazenarem comunicações de voz e dados por três anos. Além disso, o referido projeto pretende outorgar à Agência Nacional de Segurança o direito de solicitar uma chave para desencriptar toda a comunicação encriptada. Especificamente, a Seção 13(1) do projeto de lei declara:

> *Onde a Comunicação interceptada for uma Comunicação Encriptada ou Protegida, o Licenciado deverá fornecer ao Conselheiro Nacional de Segurança e ao Serviço de Segurança do Estado a chave, código ou acesso à Comunicação Protegida ou Encriptada;*

media-shutdown/463407/ (último acesso: 14 de setembro de 2016).

178 Ver Internet World Stats, http://www.Internetworldstats.com/stats1.htm (último acesso: 14 de setembro de 2016).

179 Ver Internet World Stats, http://www.Internetworldstats.com/stats1.htm (último acesso: 14 de setembro de 2016).

180 Ajibola Adigun, Affront on Freedom in Ghana with the Introduction of Spy Bill, Student For Liberty, 29 de março de 2016 https://studentsforliberty.org/africa/2016/03/29/affront-on-freedom-in-ghana-with-the-introdução da lei de espionagem/(último acesso: 14 de setembro de 2016).

181 News Gana, UN Demands Statistics on Ghana’s Spy Bill, 11 de março de 2016,https://www.newsghana.com.gh/ un-demands-statistics-on-ghanas-spy-bill/ (último acesso: 14 de setembro de 2016).

182 Nigerian Communications Commission, Draft Lawful Interception of Communications Regulations, disponível em: http://bit.ly/1du7UKO (último acesso: 14 de setembro de 2016).

Outros países da região da África Ocidental mostram um uso significativamente inferior da Internet, variando de pouco mais de 5% no Togo a mais de 20% na Costa do Marfim.[183]

África Meridional[184]

Usuários na África do Sul não estão proibidos de usar encriptação.[185] A disposição sobre tal tecnologia, entretanto, é estritamente regulada pela Lei de Comunicações Eletrônicas e Transações de 2002.[186] Os provedores de tecnologia de encriptação precisam se registrar junto ao Diretor-Geral do Departamento de Comunicações, incluindo a apresentação de perfis detalhados de pessoal confiável com responsabilidades de supervisão ou de gerência. As penas podem chegar até dois anos de prisão por qualquer violação.

Desde 2003, a Lei de Intercepção de Comunicações e Fornecimento de Informações Relacionadas à Comunicação está em vigor[187]. Essa permite à polícia exigir a desencriptação em qualquer caso de telecomunicação encriptada mediante ordem judicial. O destinatário da ordem judicial deve cumprir, fornecendo uma chave de desencriptação ou, pelo menos, auxiliar na desencriptação. As penalidades variam de dois milhões de Rand (cerca de 140 mil dólares) até dez anos de detenção, e um teto de cinco milhões de Rand (cerca de 340 mil dólares) para as empresas.

África Central

Países da África Central, como a República Democrática do Congo, a República Centro-Africana, o Gabão e Camarões ainda não dispõem de estrutura jurídica bem desenvolvida que faça frente às questões de política na Internet. A Internet continua sendo uma esfera relativamente desregulada. Não é conhecida qualquer legislação que limite o uso de mídia *online* ou proíba o uso de tecnologia de encriptação. Apenas 3% da população da República Democrática do Congo e 4% da população da República Centro-Africana são utilizadores ativos da Internet e 11% em Camarões.[188]

183 Ver Internet World Stats, http://www.Internetworldstats.com/stats1.htm (último acesso: 14 de setembro de 2016).

184 Como não foi encontrada informação relevante específica sobre os outros 4 países na região da África Austral (Botsuana, Namíbia, Lesoto e Suazilândia), a evidência apresentada refere-se apenas à África do Sul.

185 Ver Freedom House, Freedom on the Net 2015: South Africa, https://freedomhouse.org/report/freedom-net/2015/south-africa (último acesso: 14 de setembro de 2016).

186 Ver Electronic Communications and Transactions Act, 2002 nº 25 de 2002, http://www.Internet.org.za/ect_act.html (último acesso: 14 de setembro de 2016).

187 Ver Regulation of Interception of Communication and Provision of Communication-Related Information Act, Government Gazette, nº 24286, 22 de janeiro de 2003, Lei nº 70, 2002, http://www.Internet.org.za/ricpci. html (último acesso: 14 de setembro de 2016).

188 Ver Internet World Stats, http://www.Internetworldstats.com/stats1.htm (último acesso: 14 de setembro de 2016).

5 Panoramas de direitos humanos relacionados com criptografia

Instrumentos internacionais de direitos humanos sobre liberdade de expressão e privacidade

Embora uma ampla série de direitos humanos seja abordada pelas tecnologias digitais, tais direitos à liberdade de expressão (Art. 19 do Pacto Internacional sobre Direitos Civis e Políticos [PIDCP]) e o direito à vida privada (Art. 17 PIDCP) são de particular relevância para a proteção de métodos criptográficos. Ao contrário da Declaração Universal dos Direitos Humanos (UDHR), que é uma *soft law* internacional, o PIDCP (Pacto Internacional sobre Direitos Civis e Políticos) é um tratado internacional juridicamente vinculativo.[189]

O foco da análise a seguir está no sistema universal de direitos humanos. No entanto, tal análise, também se pauta em argumentos desenvolvidos para direitos regionais ou nacionais onde quer que sejam úteis.

A liberdade de expressão[190], incluindo a liberdade de informação, protege o direito das pessoas de enviar e receber ideias e informações.[191] Enquanto a manutenção de uma opinião é uma conduta passiva e uma absoluta liberdade[192], o direito à liberdade de expressão inclui as atividades de buscar, receber e transmitir informações e ideias.[193] O acesso à informação constitui um pré-requisito para a livre formação de opinião. Juntamente com a liberdade de opinião 19 (1)), art. 19 (2) é considerado "indispensável" para o autodesenvolvimento, "essencial para qualquer sociedade", e "o pilar de toda sociedade livre e democrática".[194] Frank la Rue menciona corretamente a liberdade de expressão como um “facilitador” de muitos outros direitos usufruídos pelo PIDCP.[195] Pelo direito à liberdade de expressão e informação, a matéria protegida é caracterizada por dependências mútuas: informações constituem a base para a expressão, mas a expressão igualmente produzirá e disseminará informação.[196] As restrições ao direito à liberdade de expressão só são permitidas nas condições do Artigo 19, parágrafo 3. As restrições devem ser previstas por lei e serão necessárias (a) para o respeito dos direitos ou reputação de outros ou (b) para a proteção de segurança nacional ou da ordem

189 Toby Mendel. *The UN Special Rapporteur on freedom of opinion and expression: progressive development of international standards relating to freedom of expression.* Em: McGonagle and Donders. The United Nations and Freedom of Expression and Information. Capítulo 8, p. 238.

190 Art. 19 ICCPR; Art. 32 ACHR (Arab Charter on Human Rights); Art. 13 ACHR (American Convention on Human Rights); Art. 9 ACHPR (African Charter on Human and Peoples' Rights); Art. 23 AHRD (ASEAN Human Rights Declaration).

191 Sarah Joseph e Melissa Castan, *The International Convention on Civil and Political Rights*, terceira edição, Oxford, 2013, p. 590

192 Dominic McGoldrick, *The Human Rights Committee,* Clarendon Press, 1994, p. 460

193 General Comment 34/11.

194 CCPR/G/GC/34, § 2 com referência a Marques de Morais v. Angola, 1128/2002; Benhadj v. Algeria, No. 1173/2003; Tae-Hoon Park v. República da Coreia, nº 628/1995.

195 A/HRC/17/27, § 23. Cf. Michael O'Flaherty. op cit. pp 58 et seq.

196 Tarlach McGonagle. em: McGonagle e Donders. *The United Nations and Freedom of Expression and Information.* capítulo 1, p. 3

pública ou da saúde pública ou moral. Uma possibilidade adicional de restrição é estabelecida no art. 20 do Pacto Internacional dos Direitos Civis e Políticos.[197] No contexto de limitações à criptografia, as restrições serão na maioria das vezes fundamentadas no Artigo 19, (3)(b), ou seja, riscos para a segurança nacional e à ordem pública. Isso levanta a questão complexa da relação e distinção entre segurança do indivíduo, como por exemplo de interferências em comunicações eletrônicas pessoais e na segurança nacional. Ambas não são necessariamente a mesma coisa. Existe o perigo de os governos darem ênfase à segurança nacional por conta de definições técnicas de segurança de computadores e/ou segurança humana.[198]

O Artigo 19 do PIDCP (Pacto Internacional sobre Direitos Civis e Políticos) se aplica a todas as formas de expressão audiovisuais, eletrônicas e baseadas na Internet.[199] O texto da norma é, portanto, claramente flexível para se ajustar aos avanços sóciotécnicos. O Artigo 19 protege ainda as práticas de comunicação na Internet e os diferentes tipos de serviços intermediários, não apenas os serviços que disseminam informações, mas também aqueles que permitem a comunicação.[200] A Internet possui um potencial sem precedentes de atividade comunicativa multidirecional, também em função de suas barreiras de entrada relativamente baixas e a capacidade de atores baseados na Internet ajudam a determinar a forma de liberdade de expressão e informação.[201] As funções importantes do principal moderador em debates públicos ou guardião principal, portanto, não são mais atribuídas primeiramente à mídia tradicional, embora esta ainda seja a principal fonte de conteúdo jornalístico e estabeleça a agenda de maneira mais ampla.[202]

Devido à sua importância estrutural para a liberdade de expressão, todo o processo de proteção do conteúdo jornalístico contra interferências indevidas é contemplado pelo Artigo 19. Adicionalmente, isso significa também que as limitações são apenas lícitas quando riscos específicos e iminentes para interesses públicos ou privados importantes podem ser demonstrados pelo respectivo Estado. Com base nessa avaliação, os intermediários também podem desfrutar de proteção da liberdade de expressão em razão de sua importância estrutural para os demais se comunicarem, mesmo que não estejam apresentando "declarações" próprias. Esse aspecto será detalhado abaixo, especificamente com relação à sua função de acesso à encriptação.

O direito à privacidade[203] protege contra "interferências arbitrárias ou ilegais" na privacidade do indivíduo, da família, de residências e correspondências particulares. O Artigo 17 (1) do PIDCP (Pacto Internacional sobre Direitos Civis e Políticos) protege ainda contra “ataques ilegais” contra a honra e reputação de pessoas. O

197 Manfred Nowak, CCPR Commentary, 2a edição, p. 477 Cf. Michael O’Flaherty. International Covenant on Civil and Political Rights: interpreting freedom of expression and information standards for the present and the future. Em: McGonagle and Donders. *The United Nations and Freedom of Expression and Information.* capítulo 2, p. 69 e seguintes.

198 Para mais discussão, consulte Nissenbaum 2005.

199 CCPR/C/GC/34, § 12.

200 Josef and Castan. op cit. p. 599.

201 Tarlach McGonagle. ibid. p. 5.

202 Ver Tarlach McGonagle. ibid.

203 Art. 17 ICCPR; Art. 21 ACHR (Arab); Art. 11 ACHR (America); Art. 21 AHRD.

escopo do Artigo 17 é amplo. A privacidade pode ser entendida como o direito de controlar informações sobre si mesmo.[204] A possibilidade de viver a vida como se julgar conveniente, dentro dos limites estabelecidos pela lei, depende efetivamente das informações que os outros têm sobre nós e usam para informar seu comportamento a nosso respeito. Isso faz parte da justificativa central para proteger a privacidade como um direito humano.

A disposição sobre o direito à privacidade permite novas manifestações no escopo da proteção.[205] Com efeito, o surgimento das comunicações em rede não foi previsto quando a disposição foi redigida. No entanto, o conceito de "correspondência" no n.º 1 do Artigo 17 abrange logicamente a integridade e a confidencialidade de novas formas de comunicações eletrônicas privadas, como e-mails e mensagens diretas em plataformas como o Twitter.[206] Na medida em que as comunicações eletrônicas facilitam a liberdade de procurar, acessar e transmitir informações e ideias, existe uma estreita inter-relação entre privacidade e liberdade de expressão. Do mesmo modo, quando os métodos criptográficos são utilizados para garantir a proteção da confidencialidade ou integridade de informações, reforçando assim a proteção do direito à privacidade; por conseguinte, a proteção pode ser estendida a essas novas formas de comunicação segura.[207] Somente então, pode-se falar de uma real liberdade de invasões indevidas e injustificáveis.[208]

O amparo do Artigo 17 do PIDCP também facilita a liberdade de pensamento, associação e religião (embora estes também sejam protegidos como direitos independentes). Como tal, a privacidade tem a qualidade amplamente reconhecida de possibilitar o exercício de outros direitos – uma qualidade que compartilha com o direito à liberdade de expressão. Do ponto de vista acadêmico, Volio declara que "todos os direitos humanos são aspectos do direito à privacidade",[209] uma noção reiterada por Regan.[210]

Além do dever de não infringir esses direitos, os Estados são incumbidos de garantir efetivamente o exercício da liberdade de expressão e privacidade de cada indivíduo sob sua jurisdição.[211] A Seção 2, Artigo 17 do PIDCP sobre o direito à privacidade, explicitamente ordena os Estados a protegerem os cidadãos contra interferências mediante legislação e outras medidas.[212] É necessário garantir o direito contra interferências e atentados, quer emanem de autoridades estatais, de pessoas jurídicas ou físicas.[213] É importante ressaltar que a confidencialidade e integridade das comunicações devem ser protegidas *de jure e de facto*,[214] enquanto medidas

---

204 Ver Charles Fried. Privacy. (1968) 77 *Yale Law Journal* pp. 475, 483.

205 F. Volio. Legal Personality, Privacy and the Family, p. 197, in: L. Henkin, 'The International Bill of Rights', New York: Columbia University Press 1981. This is equally true of Art. 8 of the European Convention of Human Rights, see e.g. ECtHR 4 dec. 2008, Appl. No 30562/04, §66, for an overview of protected realms including ECtHR jurisprudence

206 General Comment 16/32, §8. Manfred Nowak. op cit. p. 401.

207 Ver também Wagner 2012.

208 Cf. a definição de SE Wilborn. Revista de Direito da Geórgia 32 (1998), pp. 825, 833.

209 F. Volio. op cit. p. 193.

210 Ver Regan 1995.

211 CCPR/G/GC/34, § 11.

212 Observação de Caráter Geral 16/1.

213 Observação de Caráter Geral 16/1.

214 Nowak observa ainda que esta proteção do sigilo de correspondência e telecomunicações nos termos do Artigo 17, o PIDCP é extensível aos casos em que os sistemas de divulgação de informações são

efetivas precisam ser implementadas para assegurar que o processamento de dados pelas autoridades públicas e órgãos privados respeitem o Pacto.[215]

Ao considerar a proteção de uma determinada forma de encriptação segundo esses direitos humanos relevantes, vale a pena fazer a distinção entre a aplicação técnica da encriptação e as propriedades de comunicação, informação e computação voltadas para o ser humano. Conforme já discutido, essas propriedades abrangem confidencialidade, privacidade, autenticidade, disponibilidade, integridade e anonimato. É este conjunto de propriedades de comunicação e armazenamento de informações ou ferramentas de processamento que merece proteção contra interferências, pois essas propriedades efetuam a proteção dos direitos estabelecidos sobre a égide das leis internacionais dos direitos humanos pelos direitos humanos. Por conseguinte, o Comitê de Ministros do Conselho da Europa identificou a proibição ou o enfraquecimento da encriptação, indicando passos contrários à liberdade na Internet.[216]

A liberdade de expressão e opinião e o direito à vida privada (incluindo o direito à comunicação privada) podem entrar em conflito em situações específicas. Logo no início, reconheceu-se que as obrigações positivas previstas no Artigo 17, Seção 2 não devem resultar na autorização da censura e o fato de que o direito à privacidade e o direito à liberdade de expressão são interdependentes.[217] A liberdade de expressão pode interferir, mas tem que respeitar a proteção do direito à privacidade, quando a expressão se refere ou afeta uma pessoa física. Existe uma ligação adicional. A necessidade humana básica nos contextos de comunicação é comunicar e receber informações e desenvolver a personalidade. Para ser relevante nesse aspecto, o processo de comunicação deve cumprir certos requisitos normativos que se estendem a ambos os direitos em análise.

Como dito acima, para o exemplo da liberdade de expressão, esses direitos podem entrar em conflito com outros direitos e interesses, tais como dignidade, igualdade ou vida e segurança de um indivíduo ou interesses públicos legítimos. Em tais circunstâncias, a integridade de cada direito ou valor deve ser mantida ao máximo, e quaisquer limitações requeridas para o equilíbrio devem ser legais, necessárias e proporcionais (sobretudo, de forma menos restritiva) em vista de um objetivo legítimo (como os direitos do próximo, a moral pública e a segurança nacional).

operados por empresas privadas. Cf. M. Nowak, p. 401.

215 Observação de Caráter Geral 16/32, § 8 - § 10.

216 Recomendação CM/Rec (2016) 5 do Comitê de Ministros aos Estados Membros sobre liberdade na Internet. 13 de abril de 2016. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa, points 4.1.7. e 4.2.5.

217 MJ Bossuyt, 'Guide to the "travaux préparatoires" of the International Covenant on Civil and Political Rights', Dordrecht: Nijhof 1987, p. 346, referente à Comissão de Direitos Humanos, 9ª sessão, E/CN.4/SR.374, p. 12-15

Garantindo “comunicações irrestritas”

Com base na avaliação de Frank La Rue sobre a importância estrutural da liberdade de expressão, é importante identificar características essenciais de pré-condições legais e factuais que tornam o processo de comunicação efetivamente “livre”. Um desses requisitos essenciais, amplamente fomentado pela disponibilidade da encriptação, é o que podemos chamar de “comunicação sem restrições”. A encriptação dá suporte a esse modo de comunicação, permitindo que as pessoas protejam a integridade, disponibilidade e confidencialidade de suas comunicações. A exigência de comunicações sem restrições é uma condição importante para a liberdade de comunicação, que é reconhecida por tribunais constitucionais como o Supremo Tribunal dos Estados Unidos[218] e o *Bundesverfassungsgericht* alemão[219], bem como o Tribunal Europeu dos Direitos do Homem[220].

Mais especificamente, a comunicação substancial exige que as pessoas escolham livremente as informações e desenvolvam suas ideias, o estilo da linguagem e selecionem o meio de comunicação de acordo com suas necessidades pessoais.[221] A imposição de instrumentos de censura e seus impactos no livre exercício da liberdade de expressão ilustra os efeitos adversos sobre esses aspectos relevantes e características do direito. Fornecer conteúdo falsificado, através da interferência na segurança dos canais de divulgação, distorce o que o comunicador gostaria de transmitir. A ciência do monitoramento de comunicações por terceiros é capaz de alterar o modo de comunicação.[222] Os cidadãos podem escolher mudar seu modo de expressão, burlar censores ou até abster-se completamente de se comunicarem sobre questões específicas por meio de autocensura. Este último demonstra que o *chilling effect* pode ser visto como uma possível distorção da comunicação, caso as condições para “comunicação irrestritas” (*uninhibited*) deixem de existir.

A comunicação irrestrita é também uma condição para o desenvolvimento pessoal autônomo. Os seres humanos desenvolvem sua personalidade ao se comunicarem com outras pessoas.[223] De acordo com o primeiro relator especial da ONU sobre privacidade, o professor Joe Cannataci, a privacidade não é apenas um direito facilitador, mas também um direito essencial que possibilita a conquista de um direito fundamental abrangente ao livre desenvolvimento desimpedido de nossa personalidade.[224] Caso a comunicação seja restringida, a interação é enviesada porque uma declaração não reflete apenas as visões pessoais verdadeiras (mais internas) do interlocutor, mas podem ser indevidamente influenciadas por considerações que não deveriam moldar a comunicação. Portanto, o processo de formação da personalidade por meio da interação social é interrompido.

---

218 Ver, por exemplo, New York Times Co. v. Sullivan, 376 U.S. 254 (1964) e Dombrowski v. Pfister, 380 U.S. 479 (1965).

219 Ver BVerfG NJW 1995, 3303 (3304) e BVerfG NJW 2006, 207 (209).

220 Cumhuryiet Vafki e outros v. Turquia, CEDH 10.08.2013 - 28255/07; Ricci v. Itália, CEDH 10.08.2013 - 30210/06.

221 Cf. Observação de Caráter Geral 16/8.

222 Conforme o Comentário de Caráter Geral 34 enfatiza, existe uma inter-relação entre privacidade e liberdade de expressão. C.f. a partir de uma perspectiva americana Canes-Wrone/Dorf, Revista de Direito NYU 90 (2015), 1095 e seguintes.

223 Tarlach McGonagle. The United Nations and Freedom of Expression and Information. capítulo 1, p. 3

224 Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, A/HRC/31/64.

Os efeitos restritivos de tal interrupção afetam diretamente a livre expressão de informações e ideias de uma pessoa. Além disso, quando as condições para as comunicações irrestritas deixam de existir, pode haver influência no ambiente comunicativo e expressivo de uma sociedade como um todo. Assim, a falta de comunicações irrestritas pode resultar na estagnação da vida intelectual.[225] Esse efeito mais geral torna qualquer ação estatal que obstrua a possibilidade de comunicações irrestritas por si só uma restrição grave da liberdade de expressão. Além disso, apoia a perspectiva de que o uso da tecnologia de encriptação remete ao direito à liberdade de expressão ("direito à encriptação"). O exemplo da decisão do Tribunal Constitucional alemão sobre o "direito básico de TI"[226] apoia e ilustra a viabilidade da extensão dos direitos básicos, em vista da mudança tecnológica de maneiras semelhantes: O tribunal constitucional alemão reconhece – metaforicamente – que partes da personalidade de um indivíduo entram em sistemas de TI e, portanto, a proteção aplicada tem que percorrer o mesmo caminho.

Uma vez que as medidas estatais que restringem o uso e a implantação de encriptação tendem a ter o efeito de limitar as comunicações irrestritas, pode-se argumentar que o conceito de proteção efetiva dos direitos humanos tem que considerar a possibilidade de um cidadão se proteger por meio da tecnologia. Numa sociedade complexa, a liberdade de expressão não se torna realidade quando as pessoas têm o direito de falar. Um segundo nível de garantias precisa proteger a condição de fazer uso do direito de se expressar. Se existe o risco de vigilância, o direito de proteger uma liberdade de expressão por meio de encriptação tem que ser considerado como um desses direitos de segundo nível. Assim, a restrição da disponibilidade e eficácia da encriptação como tal constitui uma interferência na liberdade de expressão e no direito à privacidade, uma vez que protege a vida privada e a correspondência. Portanto, deve ser avaliada em termos de legalidade, necessidade e propósito.

Aspectos processuais: garantindo transparência

A liberdade de expressão e o direito à privacidade (incluindo o direito a comunicações privadas) têm um caráter substancial, isto é, protegem materialmente um determinado comportamento ou uma condição pessoal. Consta devidamente na teoria dos direitos fundamentais que os direitos substantivos devem ser complementados pelas garantias processuais para serem efetivos.[227] Essas garantias processuais podem ser direitos como, por exemplo, o direito a uma tutela efetiva. No entanto, é importante reconhecer que esses direitos processuais devem, assim como os direitos substantivos, ser acompanhados por deveres processuais específicos de governos, caso contrário tais direitos estariam comprometidos.

Os direitos civis e políticos no Pacto Internacional dos Direitos Civis e Políticos e na Declaração Universal dos Direitos Humanos são tradicionalmente, pelo menos numa primeira análise, percebidos como liberdades da interferência do Estado.[228]

---

225 Cf. Sylvie Coudray. The United Nations and Freedom of Expression and Information. capítulo 7, p. 258.
226 BVerfG NJW 2008, 822.
227 Cf. Robert Alexy e Julian Rivers. A Theory of Constitutional Rights. pp. 315 e seguintes.
228 Herdegen Völkerrecht. § 47 recital 1.

São conceituados como direitos negativos. Isso significa que eles exigem que um Estado se abstenha de certas ações. Como referido anteriormente, em certa medida, os direitos também exigem ação positiva, inclusive para proteger contra violações de direitos por parte de entidades não governamentais.[229] Certamente, o tratado PIDCP (Pacto Internacional sobre Direitos Civis e Políticos) aplica-se apenas ao Estado diretamente; portanto, é necessária uma ação ou omissão deste para invocar direitos fundamentais. Ao mesmo tempo, os Princípios Orientadores das Nações Unidas sobre Empresas e Direitos Humanos apelam aos atores privados para que respeitem os direitos humanos em suas operações.

Ao verificar as ações do Estado sob essa ótica, vale observar que em diversos campos de políticas é possível notar mudanças nos modos de governança legal. Essa governança legal não deve ser frequentemente caracterizada como uma forma linear mais tradicional de regulação entre Estado e cidadãos na relação vertical. Mas é exercida em uma rede de agentes estatais e não estatais, não tendo por base apenas normas legais, mas também instrumentos informais.[230]

Este é particularmente o caso pertinente às tecnologias e serviços de informação e comunicação no atual ambiente globalizado.

Esses mecanismos de governança em rede, incluindo instrumentos informais, podem ser altamente eficazes para atingir metas regulatórias. No entanto, do ponto de vista dos direitos humanos, eles também geram riscos. Quando os sistemas de governança se tornam cada vez mais complexos e quando os agentes estatais colaboram informalmente com agentes privados em áreas sensíveis dos direitos humanos,[231] observa-se o risco de uma difusão ou ofuscação de responsabilidades. Os cidadãos não sabem quem deve responsabilizar-se por certos efeitos ou injustiças averiguadas. Portanto, os direitos substantivos devem ser interpretados de forma, também, a prever o dever de tornar os sistemas de governança transparentes, pelo menos na medida em que permita aos cidadãos avaliarem (1) quem tomou alguma decisão e (2) quais medidas foram adotadas.

Esse aspecto é extremamente relevante para as negociações do governo com intermediários e outros *players*, em variadas jurisdições, no que diz respeito à encriptação. Essas negociações e seus resultados podem levar a um sistema em que os Estados não realizem ações formais, mas apenas recorram à cooperação com a indústria para fornecer dados ou chave de encriptação quando solicitada, e independentemente de uma avaliação de legalidade, necessidade e propósito legítimo. Uma vez que não há leis ou regulamentos eventualmente sujeitos ao escrutínio legal, o aspecto processual da proteção dos direitos humanos requer transparência (não obstante outras garantias processuais e substantivas). Os Estados têm o dever de serem transparentes sobre esses mecanismos interconectados e as restrições que impõem ao livre uso e implantação de métodos e tecnologias criptográficas seguras. O inverso obtém-se quando as denominadas "ordens de mordaça" (*gag orders*) são emitidas. Essas ordens impedem frequentemente que a indústria não só informe aos titulares de dados, mas também ao público em geral sobre interferências deliberadas em seus direitos. Nesse

229 Cf. Schiedermair. Der Schutz des Privaten als internationales Grundrecht. p. 74.
230 Ver, por exemplo, Røiseland. Informal Governance. In: Encyclopedia of Political Science, p. 1018.
231 Cf. Tarlach McGonagle. op cit. capítulo 1, p. 39

sentido, um apelo à transparência é mais do que um apelo geral para promover clareza e garantir a responsabilização. Isso constitui um pré-requisito para conhecer os perigos aos direitos fundamentais e desfrutar das respectivas liberdades.

Estados, usuários e provedores de serviços: "intermediários de segurança"

Considerando que os usuários dependem dos provedores de serviços com relação à segurança de seus dados, é importante observar a estrutura jurídica referente a esses prestadores de serviços com especial atenção, bem como do ponto de vista da proteção dos direitos humanos no domínio digital. A Seção 2 deste estudo já ilustrou a variedade de configurações em que os métodos criptográficos são potencialmente implementados com o objetivo de atender aos interesses dos usuários finais. A partir dessa visão geral, constata-se que, além da possibilidade de os usuários implantarem as próprias proteções, a efetivação da proteção dos direitos humanos requer ímpeto e envolvimento por parte dos provedores de serviços. Em relação à vigilância de usuários de serviços baseados em nuvem, em muitos aspectos "um usuário não pode se proteger, mas depende do provedor de serviços na nuvem para o exercício dos direitos fundamentais e a proteção contra interferências arbitrárias da segurança nacional".[232] Esses provedores de serviços geralmente atuam como intermediários, facilitando a expressão e a comunicação de seus usuários de diferentes tipos.[233] É preciso que os usuários possam confiar em seus provedores de serviços a fim de tomar as medidas apropriadas que garantam a integridade, disponibilidade e confidencialidade de suas informações e comunicações. Os Estados não devem, portanto, impedir a capacidade das plataformas e serviços de mídia e comunicação de usar métodos criptográficos seguros. Em vez disso, os arcabouços jurídicos devem prever obrigações para os provedores de serviços ou, pelo menos, incentivá-los nesse sentido, por exemplo, estabelecendo padrões mínimos técnicos em seus atos de proteção e segurança de dados ou estabelecer selos de segurança de dados que possam sinalizar o grau de proteção implementado para os usuários. Em qualquer caso, medidas tomadas por intermediários para proteger a privacidade de seus usuários estão no escopo tanto do Artigo 19 como do Artigo 17 do PIDCP (Pacto Internacional sobre Direitos Civis e Políticos) devido à sua importância estrutural para a proteção factual dessas liberdades.

Nos debates sobre política criptográfica, a questão do acesso legal pelo governo – e as condições sob as quais esse acesso deve ocorrer para respeitar os direitos humanos – tem um foco vertical e nacional. O que se entende aqui é que a discussão aborda os deveres e responsabilidades do Estado em relação aos membros de sua própria sociedade, e as leis e regulamentos que devem ser estabelecidos em conformidade, respeitando os direitos humanos. Em cada país, a preocupação com o acesso normalmente está concentrada na falta de acesso pelas autoridades

232 Ver Arnbak 2016.

233 MacKinnon et al. UNESCO study; Cf. Karol Jakubowicz. Early days: the UN, ICTs and freedom of expression. in: The United Nations and Freedom of Expression and Information. chapter 10, pp. 324 et seq.

competentes. O que às vezes não é reconhecido suficientemente é o fato de que os serviços e ferramentas em foco não se encerram nas fronteiras.[234] O mesmo se aplica ao governo e a outros atores que eventualmente busquem obter acesso à informação e à comunicação transnacionalmente. A dimensão internacional e a possibilidade de acesso transnacional, efetivamente, significa que os agentes estrangeiros devem ser incluídos nos modelos de ameaças para proteção de dados e políticas de segurança cibernética.[235] Esse é um dos motivos pelos quais os métodos criptográficos podem ser ativamente explorados para restringir e moldar o acesso transnacional aos dados pelos governos.

Essas complexidades de jurisdição no acesso legal do governo são significativas e apresentam um quebra-cabeça ainda não resolvido. Em particular, mudanças dramáticas vêm ocorrendo no acesso legal tradicional do governo a comunicações digitais pelo direcionamento de provedores de telecomunicações com conexões locais fortes, para acessar por meio do direcionamento para serviços *over-the-top* (OTT) direcionados com menos conexões ou conexões mais fracas nas jurisdições onde são oferecidos serviços aos usuários. Isso suscita a questão sobre em quais casos tais provedores de serviços, que operam internacionalmente, deveriam (ser capazes de) fornecer os dados e comunicações do usuário às autoridades locais. Considerações relevantes incluem a localização dos dados, o(s) respectivo(s) usuário(s) e sua nacionalidade e as especificidades jurisdicionais do assunto em análise.

A implementação da encriptação pelos provedores de serviços é um fator adicional que dificulta essa configuração. Do ponto de vista dos provedores de serviços, parece provável que os métodos criptográficos terão que ser projetados para contabilizar somente os dados do usuário com base no processo legal válido em determinadas situações. Mais especificamente, os métodos criptográficos estão cada vez mais entre os ingredientes necessários das medidas para limitar a exposição de dados e comunicações de usuários e reduzir a complexidade de atender às solicitações de acesso do governo. A encriptação ponta-a-ponta pode resultar em nenhum dado disponível a ser fornecido em resposta a requerimento legal do governo, mas a suspensão do serviço em tais casos é claramente desproporcional.

Nos últimos anos, empresas e, especialmente, intermediários *online* têm se encontrado cada vez mais no foco do debate sobre a implementação dos direitos humanos.[236] Nesse contexto, vale a pena notar que os intermediários *online*[237] não só desempenham um papel de intermediários entre provedores de conteúdo e usuários, mas também um dos "Intermediários de Segurança" em vários aspectos.

---

234 Cf. Karol Jakubowicz. Early days: the UN, ICTs and freedom of expression. in: The United Nations and Freedom of Expression and Information. chapter 10, pp. 341 et seq.

235 Ver, por exemplo, Kristina Irion. Government Cloud Computing and National Data Sovereignty. 30th June 2012. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1935859. See also Joris van Hoboken, Axel Arnbak and Nico Van Eijk. Obscured by Clouds or How to Address Governmental Access to Cloud Data from Abroad. 9th June 2013. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2276103.

236 Cf. os Princípios Orientadores das Nações Unidas sobre Empresas e Direitos Humanos. 2011. http://www.ohchr.org/ Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf e a publicação da UNESCO Fostering Freedoms Online. O Papel dos Intermediários da Internet. 2014. http://unesdoc.unesco.org/ images/0023/002311/231162e.pdf.

237 Cf. Karol Jakubowicz. Early days: the UN, ICTs and freedom of expression. in: The United Nations and Freedom of Expression and Information. chapter 10, pp. 324 et seq.

Suas práticas e padrões em relação à encriptação são altamente relevantes para o acesso e uso efetivo dessas tecnologias pelo usuário. Visto que um enorme volume de dados passa pelos seus roteadores e é armazenado em suas nuvens, esses oferecem pontos ideais de acesso para a comunidade de inteligência e agentes não estatais. Assim, eles também, talvez involuntariamente, funcionem como uma interface entre o Estado e os usuários em questões de política de encriptação. O papel também deve ser refletido no debate sobre direitos humanos, e exige uma integração abrangente da segurança da informação e comunicação do usuário no modelo emergente de governança da Internet de hoje.

Direitos humanos e criptografia: obrigações e espaço para ação

A tabela abaixo mostra os riscos específicos que poderiam ser enfrentados, bem como a adoção de soluções criptográficas pelos serviços relevantes e os requisitos mínimos e boas práticas para enfrentar esses riscos com eficácia. Os requisitos mínimos identificados neste estudo, a respeito dos direitos humanos e da política criptográfica, não são exaustivos e são oferecidos para ajudar a orientar o desenvolvimento de normas adicionais na prática em vários níveis.

Riscos	Adoção de serviços relevantes de soluções criptográficas	Boas práticas
Restrições técnicas de acesso ao conteúdo (bloqueio)	Provedores de armazenamento em nuvem	Garantir acesso autenticado ao conteúdo publicamente disponível
Interceptação	Provedor de conexão de Internet	Segurança jurídica
Hackeamento por agentes estatais e não estatais	*Sites* do editor	Transparência sobre interferências
Análise e vigilância de tráfego	Mecanismos de busca	Disponibilidade de comunicações de ponta-a-ponta seguras
Interferência na confiabilidade ou autenticidade do conteúdo	Serviços de comunicações e mensagens	Disponibilidade de acesso anônimo
	Navegadores	Educação, incluindo alfabetização midiática e informacional
		Padrões e inovação

Em casos específicos de interferência na liberdade de usar e adotar métodos criptográficos, deve-se realizar uma avaliação legal considerando as circunstâncias jurídicas, societárias e técnicas específicas, tendo em vista as normas internacionais

em matéria de direitos humanos. O conceito de Universalidade da Internet, desenvolvido pela UNESCO, incluindo sua ênfase na abertura, acessibilidade a todos e participação multissetorial, também pode ser concretizada. Embora tais requisitos mínimos e boas práticas possam basear-se em análises jurídicas mais abstratas, essas avaliações devem ser feitas em contextos específicos.

Em resumo, com alguns exemplos, várias observações podem ser feitas. O acesso autenticado seguro ao conteúdo publicamente disponível, por exemplo, constitui uma proteção contra várias formas de censura pública e privada e limita o risco de falsificação. Pode fomentar a confiança na esfera pública *online*, em serviços *online* e *e-commerce* em geral.[238] Um dos padrões técnicos mais predominantes que permite acesso autenticado seguro é o TLS. Intimamente relacionado a isso está a disponibilidade de acesso anônimo à informação. Esse acesso permite que os usuários obtenham conhecimento de qualquer área de interesse pessoal ou político sem temer repercussões ou mesmo justificar os seus interesses perante outros. Como mencionado anteriormente, o TOR é um sistema que permite a recuperação praticamente anônima de informações *online*. Ambos os aspectos do acesso ao conteúdo beneficiam diretamente a liberdade de pensamento e expressão.

O princípio da segurança jurídica é vital para todos os processos jurídicos concernentes aos métodos ou práticas criptográficas. A segurança jurídica torna os resultados previsíveis e permite que os cidadãos moldem suas ações de maneira mais consciente. Como tal, o princípio é essencial para quaisquer formas de interceptação e vigilância, pois pode evitar medos irracionais de vigilância, como quando as normas legais subjacentes são elaboradas com precisão. Assim, a segurança jurídica pode evitar *chilling effects*, reduzindo um fator-chave inibidor para o exercício dos direitos humanos.

A inovação contínua no campo da criptografia e a definição e disseminação de novos padrões técnicos também são essenciais. Os padrões criptográficos podem expirar rapidamente, à medida que a capacidade computacional aumenta continuamente. Mesmo para manter um certo nível de proteção, portanto, requer uma modernização contínua das técnicas criptográficas e sua rápida disseminação. Aqui, a educação desempenha uma função essencial para estabelecer e disseminar esses padrões, uma vez que em quase todos os casos a encriptação de informações representa um esforço que precisa ser realizado por duas ou mais partes. Os próprios usuários precisam continuar com a alfabetização midiática e informacional para se manterem a par dos problemas.

A legalidade das limitações

Demonstramos agora o escopo da proteção dos direitos humanos em relação à encriptação. No entanto, o impacto real dos direitos humanos só pode ser avaliado analisando as possíveis limitações que os Estados podem estabelecer sobre essas liberdades. A segurança nacional pode, certamente, ser um objetivo legítimo para ações que limitam a liberdade de expressão e o direito à privacidade. Contudo, as medidas devem ser necessárias e proporcionais. Se esse é o caso, só pode ser

[238] Para uma discussão aprofundada, veja a Seção 2.

avaliado individualmente. No entanto, essa análise também fornece critérios que podem se tornar bastante relevantes ao averiguar a legalidade de uma interferência estatal no direito à encriptação, como uma garantia consagrada na liberdade de expressão e na privacidade, conforme demonstrado acima. Uma interferência desse direito é especialmente grave se:

- Afetar a capacidade dos principais provedores de serviços no cenário de mídia e comunicações na proteção de informações e comunicações de seus usuários por meio de métodos e protocolos criptográficos seguros. Constituindo, assim, o requisito de comunicações sem restrições para os usuários de serviços e tecnologias de comunicação em rede.

- O Estado reduzir a possibilidade de comunidades vulneráveis e/ou agentes estruturalmente importantes, como jornalistas, de terem acesso à encriptação;

- Meros riscos teóricos e perigos impulsionarem as restrições aos direitos fundamentais pertinentes no âmbito do sistema jurídico de um estado;

- O modo de ação do Estado, por exemplo, se as restrições aos direitos fundamentais forem estabelecidas mediante acordos informais e voluntários, levar à neutralização arbitrária ou deterioração da segurança dos métodos e tecnologias criptográficas implementadas.

6 Recomendações

Recomendações gerais

É preciso reconhecer os métodos criptográficos como um elemento essencial do cenário de mídia e comunicação. O que importa, a partir da perspectiva dos direitos humanos, é que os métodos criptográficos fortaleçam os indivíduos no exercício de sua privacidade e liberdade de expressão, pois permitem a proteção de propriedades de informação, comunicação e computação voltadas para o ser humano. Estas propriedades incluem a confidencialidade, privacidade, autenticidade, disponibilidade, integridade e o anonimato da informação e comunicação.

A proteção da encriptação em instrumentos relevantes de direito e de política, sob a ótica dos direitos humanos, é especialmente importante, visto que a encriptação torna possível proteger informações e comunicações na plataforma de comunicações inseguras que seria a Internet. Inicialmente, a própria Internet não foi projetada para fornecer a segurança das informações e comunicações em geral. Ao longo dos anos, as técnicas criptográficas tornaram-se um componente central da Internet, amparadas por numerosos protocolos e padrões que apoiam a sua implementação na prática. A encriptação torna possível ajudar a garantir confidencialidade, privacidade, autenticidade, disponibilidade, integridade e anonimato em configurações específicas. Isso facilita a proteção dos direitos humanos dos usuários da Internet e a liberdade de expressão e privacidade em particular.

Seguem abaixo outras recomendações sobre as condições estruturais relacionadas à encriptação e direitos humanos:

[1] A política de encriptação deve ser vista em um contexto mais amplo de governança da Internet e de funções sociais mais amplas e valores humanos decorrentes dos vários usos da Internet.

[2] A representação do ângulo dos direitos humanos nos debates sobre a política de encriptação deve ser fortalecida. Embora influentes, na prática, outras considerações, como segurança nacional e competitividade econômica, tendem a ser fatores dominantes. Aumentar a representação do ângulo dos direitos humanos implica:

- conhecimento mais robusto de *standards* de direitos humanos e desenvolvimento de normas internacionais;
- desenvolvimento de proteções contra interferências, bem como boas práticas de agentes estatais e industriais, e de usuários;
- A necessidade de proteções contra interferências ilegais em protocolos de encriptação e implementações (incluindo *backdoors* informais, definição de padrões, etc.) e a construção de confiança no ambiente de mídia e comunicações;

- requisitos de transparência a respeito da interferência informal ilegal na segurança de mídia e comunicações;
- a promoção de práticas transparentes de código de *software* e responsabilidade na implementação de tecnologias com garantias de privacidade e segurança;
- sensibilidade ao papel da encriptação no que diz respeito à violação dos direitos das mulheres e meninas e de outros grupos vulneráveis *online*, incluindo as minorias étnicas e raciais e as comunidades LGBT;

[3] Todas as partes interessadas importantes devem estar envolvidas. A questão não é apenas relevante para o governo e a indústria, mas deve incluir também membros da sociedade civil, representantes de comunidades vulneráveis, incluindo minorias, mulheres e meninas, bem como instituições de mídia e educação.

[4] É preciso reconhecer que a encriptação não representa uma solução mágica na proteção dos direitos humanos: esta precisa ser incorporada em outros suportes e proteções para que os direitos humanos sejam efetivos.

Recomendações das partes interessadas (*Stakeholders*)

As reflexões apresentadas neste estudo levam a algumas percepções que podem ser úteis para vários interessados. As recomendações abaixo são opções a serem examinadas, projetadas para equilibrar adequadamente as questões de direitos humanos, envolvidas em outras considerações legítimas, como órgãos de aplicação da lei e segurança. As recomendações visam diferentes grupos de partes interessadas (usuários, prestadores de serviços, especialistas em tecnologia, legisladores) e o papel específico que desempenham no sistema geral.

Estados devem considerar:

[5] Não impor restrições gerais na implantação de encriptação por usuários e provedores de serviços relevantes;

[6] Incluir as considerações sobre direitos humanos em políticas de encriptação em setores relevantes e garantir que a política de encriptação leve em consideração a dimensão do gênero, bem como atenda às necessidades específicas das minorias protegidas.

[7] Estabelecer segurança jurídica – a falta de segurança jurídica pode dificultar especialmente a comunicação livre e aberta, uma vez que, nem os cidadãos nem os agentes da indústria podem realmente avaliar os riscos;

[8] Garantir transparência – acordos especialmente informais entre o governo e os agentes da indústria podem implicar riscos para os direitos humanos na área de encriptação, já que isso compromete a atribuição de atos aos governos, o que é uma pré-condição para aplicar os direitos humanos com maior eficácia;

[9] Assegurar a formulação de políticas baseadas em fatos (e não com base no receio) em questões de acesso governamental legítimo e envolver todas as comunidades relevantes nessas questões;

[10] Empenhar-se em prol de uma melhor coordenação internacional em questões de política de encriptação;

[11] Estimular a pesquisa e o desenvolvimento de inovação criptográfica e padrões para implantação no cenário de mídia e comunicações;

[12] Desenvolver sistemas globais de monitoramento e medição para avaliar a adoção (e a falta dela) de tecnologias que protegem as comunicações e informações do usuário;

[13] Ponderar o conceito de “Universalidade e Conhecimento da Internet” da UNESCO, incluindo processos multissetoriais para discutir como qualquer limitação na encriptação terá impacto sobre os direitos humanos, abertura e acessibilidade a todos na Internet.

O setor privado e os intermediários da Internet poderiam considerar:

[14] Os intermediários *online* não têm apenas o papel de intermediários entre provedores de conteúdo e usuários, mas também devem ser reconhecidos como "intermediários de segurança" em vários aspectos;

[15] Continuar a implementar todas as medidas de segurança adequadas que ajudem a estabelecer e promover o exercício da privacidade e da liberdade de expressão dos usuários, incluindo a encriptação de ponta-a-ponta das comunicações e o uso de encriptação autenticada para dados em repouso;

[16] participar internacionalmente e em diferentes jurisdições, de maneira a atingir um resultado de alto nível no tocante à proteção exercida pelos usuários, e não de um nivelamento por baixo;

[17] inovar na aplicação de métodos criptográficos para proteger a privacidade e a liberdade de expressão dos usuários;

[18] contribuir para o desenvolvimento aberto de tecnologias de aprimoramento da privacidade e projetos de encriptação orientados para os direitos humanos;

[19] promover práticas seguras de codificação e aumentar os esforços para melhorar a confidencialidade e o anonimato nos serviços;

[20] aumentar esforços de coordenação e contribuições para a padronização perante os desafios de fragmentação no ecossistema de software.[239]

Os usuários, a sociedade civil e a comunidade técnica poderiam considerar:

Em muitos países, pesquisas mostram a relevância que vários usuários atribuem a questões de privacidade. Consequentemente, ficam frustrados, e até mesmo hostis, quando descobrem que sua confiança na privacidade do serviço *online* pessoal e profissional foi traída. No entanto, a maioria dos usuários poderá não investir no aprimoramento da privacidade, usando os meios disponíveis de encriptação. Pesquisas indicam que isso pode ser melhor entendido como um sinal de resignação do que um sinal de que os usuários não atribuem valor à sua privacidade.

A discrepância indicada não pode ser observada apenas em relação à tecnologia criptográfica, mas também a outros meios de proteção da privacidade. Tendo isso em vista, recomendamos a seguinte abordagem:

[21] A proteção da privacidade não deve se basear apenas nos usuários que fazem uso de tecnologias criptográficas. Comunicar os riscos e difundir o conhecimento sobre as tecnologias deve fazer parte de uma política nacional, com sensibilidade suficiente para conscientizar todos os usuários, incluindo vários grupos com diferentes vulnerabilidades, tais como jornalistas, mulheres e meninas,

239 Ver Berkman Center 2016 ("Os ecossistemas de software tendem a ser fragmentados. Para que a encriptação se torne ampla e abrangente, muito mais coordenação e padronização do que existe atualmente seria necessária").

minorias, etc. Os Estados devem ser incentivados a tornar o conhecimento sobre a encriptação parte de sua comunicação, bem como programas de alfabetização midiática e informacional. Mesmo que essas medidas sejam limitadas em seus efeitos, elas continuam a constituir um elemento importante de qualquer política que coloque o usuário informado como elemento central.

[22] O desenvolvimento de tecnologias inteligentes que tornem a encriptação o mais conveniente possível apoiaria a privacidade e a liberdade de expressão, incluindo medidas especiais de proteção para jornalistas, agentes da mídia e usuários vulneráveis, como mulheres e meninas e minorias. Sistemas que saibam quando é necessário um nível mais alto de encriptação e reajam automaticamente a essa demanda podem ser úteis. Os usuários podem não querer decidir novamente sobre a segurança de suas comunicações, mas podem fazê-lo ao optar por um dispositivo ou um sistema de software.

[23] Quando os interesses dos consumidores estão em risco, pode ser eficaz não apenas contar com o usuário individual, mas fortalecer as agências que protegem os interesses dos consumidores.

[24] A política de privacidade deve ter como alvo os intermediários que atendem os usuários em suas comunicações e transações. Se houver encriptação efetiva nesse nível, até mesmo os usuários que não perceberem os riscos estarão protegidos.

[25] Há um papel importante para a educação e capacitação, e o objetivo mais geral de que as pessoas tenham uma ideia realista dos riscos que enfrentam sem estarem sobrecarregados com requisitos impossíveis de se protegerem contra o acesso não autorizado ao seu conteúdo e comunicações. Ações nesse sentido podem se basear em pesquisas sobre os motivos para não usar encriptação.[240]

[26] Questões de gênero e comunidades vulneráveis: mulheres e meninas, bem como jornalistas, agentes de mídia e minorias protegidas, podem estar mais expostos a interferências nos direitos humanos e, portanto, ainda com maior necessidade de comunicações encriptadas e de aprimoramento específico em seus problemas.

[27] O debate sobre direitos humanos pode se beneficiar enormemente da *expertise* fornecida pela comunidade técnica. Assim, o envolvimento de especialistas em tecnologia deve ser bem-vindo. Especialistas em tecnologia devem considerar os efeitos de suas decisões sobre privacidade e liberdade de comunicação. Essas considerações devem estar refletidas na ética profissional e no treinamento.

[28] A definição de padrões de processos de comunidades com base multissetorial para a promoção dos direitos humanos nas normas técnicas deveriam ser apoiadas e reforçadas. Esforços devem ser priorizados para melhorar rapidamente protocolos conhecidos por serem inseguros.

---

240 EgK Renaud, M. Volkamer, A. Renkema-Padmos.

Referências

Harold Abelson et al. *Keys Under Doormats: mandating insecurity by requiring government access to all data and communications*. Julho de 2015. Disponível em: http://www.crypto.com/papers/ Keys_Under_Doormats_FINAL.pdf.

Access and PEN American Center. *Comment on Encryption/Anonymity*. UN, 2015.

Bhairav Acharya. *The Short-lived Adventure of India's Encryption Policy*. Dezembro de 2015. Disponível em: https://www.ocf.berkeley.edu/~bipla/the-short-lived-adventure-of-indias-encryption- policy/.

ACLU, Stingray. *Tracking Devices: Who's Got Them?* Disponível em: https://www.aclu.org/map/stingray- tracking-devices-whos-got-them (last accessed: 29 August 2016).

Ben Adida et al. *CALEA II: Risks of Wiretap Modifications to Endpoints*. Center for Democracy & Technology, 17 May 2013, Disponível em: https://www.cdt.org/files/pdfs/ CALEAII-techreport.pdf

Marion Albers. *Informationelle Selbstbestimmung*. Baden-Baden 2005.

Robert Alexy and Julian Rivers. *A Theory of Constitutional Rights*. Oxford, 2010.

Apuzzo et al. A*pple and Other Tech Companies Tangle with U.S. Over Data Access*. New York Times, Setembro de 2015.

Axel Arnbak. *Securing Private Communications: Protecting Private Communications Security in E.U. Law: Fundamental Rights, Functional Value Chains and Market Incentives*. Kluwer Law International, 2016.

Kim Arora. *Draft National Encryption Policy put up online for public comment, experts worried*. The Times of India, Setembro de 2015.

Aydin et al. *Turkey v. encryption: An attack on freedom of expression*. Access, Setembro de 2015.

Jack Balkin. *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*. NYU Law Review 79, 2004.

Derek Bambauer. *Orwell's Armchair*. The University of Chicago Law Review 79, 2012.

BBC. *MI5 boss warns of technology terror risk*. BBC UK, Setembro de 2015.

Cory Bennett and Katie Bo Williams. *Paris revives battle over government access to encrypted data*. The Hill, Novembro de 2015.

Berkeley Information Privacy Law Association Blog. *The Short-lived Adventure of India's Encryption Policy.*

Berkman Center. *Don't Panic: Making Progress on the "Going Dark" Debate*. Fevereiro de 2016.

Daniel Bernstein, Tanja Lange and Ruben Niederhagen. *Dual EC: A Standardized Back Door.* Cryptology ePrint Archive, 2015.

Thomas Böckenförde. *Auf dem Weg zur elektronischen Privatsphäre*. 2008.

Markus Böhm. *Messenger Telegram: Lieblings-App der IS-Terroristen sperrt Propagandakanäle.* Novembro de 2015. Disponível em: http://www.spiegel.de/netzwelt/apps/is-auf-telegram-messenger-app-kuendigt-massnahmen-an-a-1063535.html.

Gabriele Britz, *Vertraulichkeit und Integrität informationstechnischer Systeme*. DÖV 2008.

Bernard Cazeneuve. *French Minister of the Interior Speech at the Joint Press Conference with Thomas de Maizière, German Minister of the Interior*. Paris, Agosto de 2016. Disponível em: http://www.interieur.gouv.fr/Le-ministre/Interventions-du-ministre/Initiative-franco- allemande-sur-la-securite-interieure-en-Europe

Collin Anderson. *The Need for Democratization of Digital Security Solutions to Ensure the Right to Freedom of Expression*: *Joint Submission to the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Mr. David Kay*. Fevereiro de 2015. Disponível em: http://www.ohchr.org/Documents/Issues/Opinion/Communications/CitizenLab.pdf.

James Comey. *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?* Outubro de 2014. Disponível em: https://www.fbi.gov/news/speeches/ going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

CTITF. *Countering the Use of the Internet for Terrorist Purposes – Legal and Technical Aspects*. Maio de 2011.

Michael Chertoff e Tobby Simon. *The Impact of the Dark Web on Internet Governance and Cyber Security*. Global Commission on Internet Governance Paper Series: No. 6. Chatham House, Fevereiro de 2015.

CoE Research Devision. *National security and European case-law, CoE*. European Court of Human Rights, 2013.

CoE Parliamentary Assembly. *Committee on Legal Affairs and Human Rights, Rapporteur: Mr Pieter Omtzigt, Report;* on Mass Surveillance, Doc. 13288. Março de 2015.

Joseph Cox. *Apple's iMessage Defense Against Spying Has One Flaw*. Wired, setembro de 2015. Disponível em: http://www.wired.com/2015/09/apple-fighting-privacy-imessage-still-problems/.

Ryan Calo. *Tech companies may be our best hope for resisting government surveillance*. Fusion, Setembro de 2015.

Canes-Wrone, Brandice Dorf, Michael C. *Measuring the chilling effect*. NYU Law Review 90, 2015.

Conner-Simons. *CSAIL report: Giving government special access to data poses major security risks*. MIT News, Julho de 2015.

Data Security Council of India e NASSCOM. *Recommendations for Encryption Policy.*

Laura DeNardis. *Hidden Levers of Internet Control, Information, Communication & Society*. 2012.

Claudia Diaz, Omer Tene e Seda Gürses. *Hero or Villain: The Data Controller in Privacy Law and Technologies*. Ohio State Law Journal, 2013.

The Economist. *The TSA Locked out*. Setembro de 2015.

EFF. *Anonymity and Encryption, Comments submitted to the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*. Fevereiro de 2015.

EFF. *EFF's Encrypt the Web Report*. Novembro de 2014. Disponível em: https://www.eff.org/encrypt-the-Web report.

EFF. *Secure Messaging Scorecard*. Novembro de 2015. Disponível em: https://www.eff.org/secure- messaging-scorecard.

ENISA e Europol. *On lawful criminal investigation that respects 21st Century data protection*. Europol and ENISA Joint Statement. Maio de 2016.

Martin Eifert. *Informationelle Selbstbestimmung im Internet*. Das BVerfG und die Online- Durchsuchungen, 2008.

EPIC. *Use of encryption and anonymity in digital communications*. UN, Fevereiro de 2015.

EPRS, Science and Technology Options Assessment (STOA). *Mass Surveillance, Part 1 - Risks and opportunities raised by the current generation of network services and application*. 2014.

EPRS, Science and Technology Options Assessment (STOA). *Mass Surveillance, Part 2 – Technology foresight, options for longer term security and privacy improvements*. 2014.

European Parliament Resolution. *Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries*, 2014/2232(INI) [Marietje Schaake Rapporteur]. Setembro de 2015.

Europol. *The Internet Organized Crime Threat Assessment (IOCTA).* Setembro de 2015. Disponível em: https://www.eurInternet.com/crime-threat-assessment-iocta-2015.

Ed Felten. *On Security Backdoors, Freedom to Tinker*. Setembro de 2013. Disponível em: https://freedom- to-tinker.com/blog/felten/on-security-backdoors/.

Ed Felten. *Software backdoors and the White House NSA panel report, Freedom to Tinker*. Dezembro de 2013. Disponível em: https://freedom-to-tinker.com/blog/felten/software-backdoors-and- the-white-house-nsa-panel-report/.

Kristin Finklea. *Dark Web*. CRS Report, Julho de 2015.

Jim Finkle. *Advanced iOS virus targeting Hong Kong protestors -security firm*. Boston, setembro de 2014. Disponível em: http://www.reuters.com/article/hongkong-china-cybersecurity-apple-idUSL2N0RV2D320140930.

FOSS. *Cryptography is Important to the Public Interest*. 2015.

Tom Fox-Brewster. *Facebook opens up to anonymous Tor users with. onion address*. The Guardian, Outubro de 2014. Disponível em: http://www.theguardian.com/technology/2014/oct/31/ facebook-anonymous-tor-users-onion.

Charles Fried. *Privacy*. Yale Law Journal 77, 1968.

Kevin Gallagher. *Why aren't more news organizations protecting their e-mail with STARTTLS encryption?* Fevereiro de 2015. Disponível em: https://freedom.press/blog/2015/02/why-arent-more- news-organizations-protecting-e-mail-with-starttls.

Eric Geller. *A complete guide to the new 'Crypto Wars'*. The Daily Dot, Abril de 2016. Disponível em: http://www.dailydot.com/politics/encryption-crypto-wars-backdoors-timeline- security-privacy/.

Julia Gerhards. *(Grund-)Recht auf Verschlüsselung?* Baden-Baden, 2010.

Samuel Gibbs. *Google can unlock some Android devices remotely, district attorney says*. The Guardian, Novembro de 2015. http://www.theguardian.com/technology/2015/ nov/24/google-can-unlock-android-devices-remotely-if-phone-unencrypted.

Andy Greenberg. *Cops Don't Need a Crypto Backdoor to Get Into Your iPhone*.

Outubro de 2015. Disponível em: http://www.wired.com/2015/10/cops-dont-need-encryption-backdoor-to-hack- iphones/.

Graham Greenleaf. *Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority, 133*. *Privacy Laws & Business International Report*, Fevereiro de 2015.

GNI. *Submission to the UN*, 2015.

Peter Gola e Rudolf Schomerus. *Bundesdatenschutzgesetz*, Munich 2015.

Dan Goodin. *Low-cost IMSI catcher for 4G/LTE networks tracks phones' precise locations*. ArsTechnica, Outubro de 2015. Disponível em: http://arstechnica.com/security/2015/10/low-cost-imsi- catcher-for-4glte-networks-track-phones-precise-locations/.

Jennifer Granick. *Federal Judge shines a spotlight on the "going dark" debate*. The Center for Internet and Society, Outubro de 2015. Disponível em: http://cyberlaw.stanford.edu/blog/2015/10/federal- judge-shines-spotlight-%E2%80%9Cgoing-dark%E2%80%9D-debate.

Apar Gupta. *How many bits are enough? the legality of encryption*. Novembro de 2011. Disponível em: http:// www.iltb.net/2011/11/how-many-bits-are-enough-the-legality-of-encryption/.

Seda Gürses e Bart Preneel. *Cryptology and Privacy*. In: Van Der Sloot, Broeders e Schrijvers (eds.). *Exploring the Boundaries of Big Data*, Netherlands Scientific Council for Government Policy, 2016.

Heninger e Halderman. *Tales from the Crypto Community: The NSA Hurt Cybersecurity. Now It Should Come Clean*, Foreign Affairs, Outubro de 2013.

Ryan Henry, Stacie Pettyjohn e Erin York. *Portfolio Assessment of Department of State Internet Freedom Program*. RAND National Security Research Division, Fevereiro de 2014. Disponível em: http://www.rand.org/content/dam/rand/pubs/working_papers/WR1000/WR1035/ RAND_WR1035.pdf.

Matthias Herdegen. *Völkerrecht*. 2014.

Alex Hern. *Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim*. The Guardian, Julho de 2015. Disponível em: http://www.theguardian.com/technology/2015/jul/06/ hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim.

Joris van Hoboken, Axel Arnbak e Nico Van Eijk. *Obscured by Clouds or How to Address Governmental Access to Cloud Data from Abroad*. Junho de 2013. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2276103.

Thomas Hoeren e Ulrich Sieber. *Handbuch Multimedia-Rech.* 2012.

Wolfgang Hoffmann-Riem. *Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*. JZ, 2008.

Jeanette Hofmann. *Constellations of Trust and Distrust in Internet Governance*. In: *Report of the Expert Group 'Risks of Eroding Trust - Foresight on the Medium-Term Implications for European Research and Innovation Policies (TRUSTFORESIGHT)*. European Commission, 2015.

Gerrit Hornung. *Die Krypto-Debatte: WIederkehr einer Untoten*. MMR 2015.

Gerrit Hornung. *Ein neues Grundrech.* CR 2008.

Human Rights Watch & ACLU. *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy*. 2014.

India Law and Technology Blog. *How many bits are enough? The legality of encryption*. India Law and Technology Blog, Novembro de 2011. Disponível em: http://www.iltb.net/2011/11/how-many-bits- are-enough-the-legality-of-encryption/.

India Telecom Laws and Regulations Handbook, 2013. Volume 1.

Indian National Telecom Policy of 1999. Disponível em: http://www.dot.gov.in/telecom-polices/new- telecom-policy-1999.

Indian National Telecom Policy of 2012. Disponível em: http://www.dot.gov.in/sites/default/files/NTP- 06.06.2012-final.pdf.

Indian Government Draft Policy, Setembro de 2015. Disponível em: http://www.scribd.com/doc/282239916/ DRAFT-NATIONAL-ENCRYPTION-POLICY.

Kristina Irion. *Government Cloud Computing and National Data Sovereignty*. Junho de 2012. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1935859.

Inserra et al. *Encryption and Law Enforcement Special Access: The U.S. Should Err on the Side of Stronger Encryption*. Heritage Foundation, 2015.

International Journal of Computer Application. *Legal Issues Involving Cryptography In India. Internet Architecture Board (IAB), Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement*. Agosto de 2015. Disponível em: http://tools.ietf.org/html/rfc7624.

Sarah Joseph e Melissa Castan. *The International Convention on Civil and Political Rights*. Oxford, 2013.

David Kaye. *Phone Encryption: Balancing Privacy and Protection, Letter to the*

Editor. NYTimes, Agosto de 2015.

David Kaye. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. Maio de 2015. Disponível em: http://www.ohchr.org/EN/HRBodies/ HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc.

Eric King e Matthew Rice. *Behind the curve: When will the UK stop pretending IMSI catchers don't exist?* Novembro de 2014. Disponível em: https://www.privacyinternational.org/node/454.

Nadim Kobeissi. *On Encryption and Terrorists*. Novembro de 2015.

Neal Koblitz e Alfred Menezes. *A Riddle wrapped in an Enigma*. Dezembro de 2015. Disponível em: http:// eprint.iacr.org/2015/1018.pdf.

Alexander Koch. *Grundrecht auf Verschlüsselung?*. CR 1997.

Eitan Konigsburg. *Embracing HTTPS*, novembro de 2014. Disponível em: http://open.blogs.nytimes. com/2014/11/13/embracing-https/.

Bert-Jaap Koops. *Crypto Law Survey - Overview per country*. Fevereiro de 2013.

Joshua Kopstein. *FBI Chief Asks Tech Companies to Stop Offering End-to-End Encryption*. Dezembro de 2015. Disponível em: http://motherboard.vice.com/read/fbi-chief-asks-tech-companies-to-stop-offering-end-to-end-encryption.

Christopher Kuner. *We actually lost the crypto wars*. LSE Media Policy Project, novembro de 2014. Disponível em: http://blogs.lse.ac.uk/mediapolicyproject/2014/11/12/we-actually-lost-the-crypto- wars/.

Micah Lee. *Apple still has plenty of your data for the feds*. The Intercept, setembro de 2014. Disponível em: https://theintercept.com/2014/09/22/apple-data/.

Julian von Lucius. *GMail ist ein Telekommunikationsdienst im Sinne des TKG*. Dezembro de 2015. Disponível em: http://www.noerr.com/de/presse-publikationen/News/gmail-ist-ein- telekommunikationsdienst-im-sinne-des-tkg.aspx.

Jonathan Mahler. *Who Spewed That Abuse? Anonymous Yik Yak App Isn't Telling*. N. Y. Times. Março de 2015.

Rebecca Mackinnon et al. *Fostering Freedom Online: The Role of Internet Intermediaries*. UNESCO/Internet Society, 2014.

McConnell, Chertoff, et al. *Why the fear over ubiquitous data encryption is overblown*. Opinion, WaPo, Julho de 2015.

Kieran MacCarthy. *Dutch govt says no to backdoors, slides $540k into OpenSSL without breaking eye contact*. The Register, janeiro de 2016.

Dominic McGoldrick. *The Human Rights Committee*. Clarendon Press, 1994.

Tarlach McGonagle e Yvonne Donders. *The United Nations and Freedom of Expression and Information*. Cambridge University Press, 2015.

McSweeney. *Worried About Your Data Security? How Encryption Can Help Protect Your Personal Information*. Huff Post, Setembro de 2015.

Amir Mizroch. *Surveillance and Silicon Valley Are 'Destroying' Europe's Privacy Balance*. Dezembro de 2015. Disponível em: http://blogs.wsj.com/digits/2015/12/11/surveillance-silicon-valley- destroying-europes-privacy-balance.

Peter Münch. *Technisch-organisatorischer Datenschutz*. 2010.

Ellen Nakashima. *FBI chief: Terrorist group turning to encrypted communications*. WaPo, Julho de 2015.

Ellen Nakashima. *Obama faces growing momentum to support widespread encryption*. WaPo, Setembro de 2015.

Michael Nelson. *Clinton, clipper and crypto*. The Hill, Setembro de 2015.

Helen Nissenbaum. *Where computer security meets national security*. *Ethics and Information Technology*, 2005.

Manfred Nowak. *CCPR Commentary*. 2nd edition, 2005.

NSC draft options paper on strategic approaches to encryption. 2015. Disponível em: http://apps. washingtonpost.com/g/documents/national/read-the-nsc-draft-options-paper-on- strategic-approaches-to-encryption/1742/.

OECD. *Cryptography Policy*. *The Guidelines and the Issues*, 1998.

A. Parvathy, Ravi Shankar Choudhary e Vrijendra Singh. *Legal Issues Involving Cryptography in India*. Abril de 2013. Disponível em: http://rspublication.com/ijca/april13/6.pdf.

Andrea Peterson. *Washington Post starts to automatically encrypt part of Web site for visitors*. WaPo, Junho de 2015.

Andreas Pfitzmann. *Datenschutz durch Technik, DuD 1999, pp. 405-408. Andreas Pfitzmann and Marit Hansen, 'Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology'.* Dezembro de 2005.

Jörg Pohle. *Das Scheitern von Datenschutz by Design: Eine kurze Geschichte des*

Versagens. FlfF-Kommunikation.

Isabelle de Pommereau. *In Snowden's wake, crypto-startups take root in Germany*. CS Monitor, Agosto de 2015. Disponível em: http://www.csmonitor.com/World/Passcode/2015/0803/In- Snowden-s-wake-crypto-startups-take-root-in-Germany.

Privacy International. *Article 19 & IHRC, Securing Safe Spaces Online*. 2015.

Privacy International. *Submission to the UN Special Rapporteur on freedom of expression – anonymity and encryption in digital communications*. Fevereiro de 2015.

Public Intelligence. *India Draft National Encryption Policy*. Setembro de 2015.

Nandagopal Rajan. *Encryption Policy: WhatsApp, Web services out of draft encryption policy after outcry*. Setembro de 2015. Disponível em: http://indianexpress.com/article/technology/tech-news- technology/draft-national-encryption-policy-you-might-need-to-store-whatsapp- messages-for-90-days/.

OECD. *OECD Guidelines for Cryptography Policy*. Março de 1997.

P. Regan. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: University of North Carolina Press, 1995.

Philipp Rogaway. *The Moral Character of Cryptographic Work*. University of California, Dezembro de 2015.

Sasha Romanosky, Martin C. Libicki, Zev Winkelman e Olesya Tkacheva. *Internet Freedom Software and Illicit Activity, Supporting Human Rights Without Enabling Criminals*. Rand Corporation, 2015.

Philipp Roos. *Das IT-Sicherheitsgesetz*. MMR, 2015.

Alexander Roßnagel. *Das De-Mail-Gesetz*. NJW, 2011.

Alexander Roßnagel. *Schriftliche Stellungnahme zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)*. Deutscher Bundestag, Innenausschuss, Ausschussdrucksache 18(4)(284)B.

Ira Rubinstein e Joris van Hoboken. *Privacy and Security in the Cloud*. Maine Law Review, 2014.

Ira Rubinstein e Michael Hintze. *Export Controls on Encryption Software*. Disponível em: http://encryption_ policies.tripod.com/us/rubinstein_1200_software.htm.

Fabian Scherschel. *Keeping Tabs on WhatsApp's Encryption*. C't, Abril de 2015.

Disponível em: http://m. heise.de/ct/artikel/Keeping-Tabs-on-WhatsApp-s-Encryption-2630361.html.

Stephanie Schiedermair. *Der Schutz des Privaten als internationales Grundrecht*. Tübingen, 2012.

Bruce Schneier. *How We Sold Our Souls - and More - to the Internet Giants*. Maio de 2015. Disponível em: https:// www.schneier.com/essays/archives/2015/05/how_we_sold_our_soul.html.

Sebastian Schulz. *Privacy by Design*. CR, 2012.

Spiros Simitis. *Bundesdatenschutzgesetz*. Baden-Baden, 2014.

Chris Soghoian. *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*. 8 J. *On Telecomm. and High Tech*. Law 359, 2009.

Oliver Stiemerling e Jürgen Hartung. *Datenschutz und Verschlüsselung*. CR, 2012.

Thomas Stögmüller. *Vertraulichkeit und Integrität informationstechnischer Systeme in Unternehmen*. CR, 2008.

Peter Swire. *Senate Judiciary Committee Hearing, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy*". Julho de 2015.

Peter Swire. *Encryption and Globalization, Columbia Science and Technology Law Review*, Vol. 23, 2012. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960602.

Jürgen Taeger e Detlev Gabel. *BDSG und Datenschutzvorschriften des TKG und TMG*. Nordstrand, 2013.

Paul Taylor. *Security that makes spies feel insecure*. Financial Times, Agosto de 2010. Disponível em: http://www.ft.com/intl/cms/s/0/7ad48c10-9e5d-11df-a5a4-00144feab49a. html#axzz3R5nCIW6I.

Telecom Regulatory Authority of India. *Recommendations on Application Services.*

Telecom Regulatory Authority of India. *TRAI Consultation paper on Mobile Financial Services*.

The Indian Express. *Needed clear, robust encryption policy – without a backdoor.*

The Internet Association. *Statement on Encryption*. Novembro de 2013.

The Reserve Bank of India. *Report of the Working Group on Electronic Banking.*

The Reserve Bank of India. *Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds.*

Thomas et al. *May seeks backing for surveillance laws*. Financial Times, 2015.

UCI Law International Justice Clinic. *Selected References: Unofficial Companion to Report of the Special Rapporteur (A/HRC/29/32) on Encryption, Anonymity and the Freedom of Expression*, 2015.

UNESCO. *Keystones to foster inclusive Knowledge Societies*. 2015. Disponível em: http://unesdoc. unesco.org/images/0023/002325/232563E.pdf.

UN Counter-Terrorism Implementation Task Force (CTITF). *Countering the Use of the Internet for Terrorist Purposes*. CTITF Working Group Report, Fevereiro de 2009.

US Department of Commerce (Bureau of Industry and Society). *Encryption Export Controls: Revision of License Exception ENC and Mass Market Eligibility.*

Vance et al. *When Phone Encryption Blocks Justice*. NYTImes, Opinion Pages, Agosto de 2015.

Andreas Voßhoff e Peter Büttgen. *Verschlüsselung tut Not*. ZRP, 2014.

W3C. *EndtoEnd Encryption and the Web*. W3C TAG Finding, Julho de 2015.

Ben Wagner. *After the Arab spring: New paths for human rights and the Internet in European Foreign Policy, European Parliament, Directorate-General for External Policies*. Policy Department, 2012.

Jane Wakefield. *How does IS communicate securely?* BBC News. Novembro de 2015.

Fabian Warislohner. *Tatort: Verschlüsselung*. *Die Schuldfrage nach Paris*. Novembro de 2015. Disponível em: https://netzpolitik.org/2015/tatort-verschluesselungstechnik-die-schuldfrage-nach-paris.

Nicholas Weaver. *We think encryption allows terrorists to hide. It doesn't.* Dezembro de 2015. Disponível em: https://www.washingtonpost.com/news/in-theory/wp/2015/12/14/we-think-encryption-allows-terrorists-to-hide-it-doesnt.

Daniel Weitzner. *Encryption solution in wake of Paris should come from Washington not Silicon Valley*. Washington Post, Novembro de 2015.

WhatsApp. *WhatsApp Encryption Overview*. Technical White Paper, Abril de 2016.

Tom Whitehead. *Internet firms to be banned from offering unbreakable encryption under new laws*. The Telegraph, Novembro de 2015.

White House. *National Security Council, Review of Strategic Approaches to Encryption, Leaked Draft Memo*. Setembro de 2015.

Zack Whittaker. *Kazakhstan will force its citizens to install Internet backdoors*. ZDNet, Dezembro de 2015.

SE Wilborn. *Revisiting the Public/Private Distinction*. Georgia Law Review 32, 1998.

Wilson Center Symposium. *How Have We Changed? Evolving Views in the U.S. on Security and Liberty. Remarks of Bob Litt.* Disponível em: https://www.youtube.com/watch?list=PLzM1iiQhVrdHHZPSZ1z_ztTrUuRPMUtRb&v=PWj8eqKKB64.

Wittes. *Thoughts on Encryption and Going Dark: Part I, Lawfare*. Julho de 2015.

Wittes. *Thoughts on Encryption and Going Dark: Part II, Lawfare.* Julho de 2015.

World Wide Web Foundation et al. *Freedom of Expression, Encryption, and Anonymity: Civil Society and Private Sector Perceptions*, 2015.

Yulong Zou, Xianbin Wang e Lajos Hanzo. *A survey on wireless security: technical challenges, recent advances and future trends, Proceedings of the IEEE.* Maio de 2015. Disponível em: http:// arxiv.org/pdf/1505.07919.pdf.

Apêndice 1: Documento Final da UNESCO *Connecting the Dots*

United Nations Educational, Scientific and Cultural Organization

CONNECTING THE DOTS: OPTIONS FOR FUTURE ACTION

Documento final

O “CONNECTing the Dots: Opções para a Ação Futura” Conferência realizada na UNESCO Sede 3 - 4 de março de 2015;

Observou o potencial da Internet para avançar o progresso humano em direção às Sociedades do Conhecimento inclusivas, e o importante papel da UNESCO na promoção desse desenvolvimento dentro do amplo ecossistema de agentes;

Afirmou os princípios de direitos humanos que sustentam a abordagem da UNESCO sobre as questões relacionadas à Internet, especificamente que os mesmos direitos que as pessoas têm *offline* devem ser protegidos *online*, conforme a resolução A/HRC/RES/26/13 do Conselho de Direitos Humanos;

Reiterou a Resolução 52 da 37ª sessão da Conferência Geral, que determinou um estudo consultivo multissetorial com opções a serem apreciadas pelos Estados-membros e comunicado à 38ª Conferência Geral no âmbito do trabalho da UNESCO sobre a Cúpula Mundial sobre a Sociedade da Informação;

Reiterou ainda o estabelecimento de princípios em documentos orientadores que contemplam os artigos 12 e 19 da Declaração Universal dos Direitos Humanos, e os artigos 17 e 19 do Pacto Internacional sobre Direitos Civis e Políticos;

E, tendo *revisado* o esboço do estudo consultivo da UNESCO,

Recomendamos o trabalho continuado sobre as opções relacionadas abaixo, e esperamos as respectivas deliberações dos Estados-membros da UNESCO sobre as mesmas:

1. Opções abrangentes da UNESCO

    1.1 Considerando a Declaração Final da primeira conferência da

WSIS+10, endossada pela 37ª Conferência Geral, afirma o valor contínuo dos resultados da Cúpula Mundial sobre a Sociedade da Informação (CMSI), incluindo o *Internet Governance Forum* (IGF), para a agenda de desenvolvimento pós-2015, questões de governança da Internet e o papel e trabalho da UNESCO;

1.2 Afirma que os direitos humanos fundamentais à liberdade de opinião e expressão e seu corolário da liberdade de imprensa e o direito de acesso à informação, o direito à reunião pacífica e o direito à privacidade, são facilitadores da agenda de desenvolvimento pós-2015;

1.3 Também afirma que aumentar o acesso à informação e ao conhecimento em toda a sociedade, assistido pela disponibilidade de informação e tecnologias de comunicação (TICs), contribui para o desenvolvimento sustentável e melhora a vida das pessoas;

1.4 Promover o alinhamento de leis, políticas e protocolos relacionados à Internet com a legislação internacional de direitos humanos;

1.5 Apoiar os princípios de Universalidade da Internet (ROAM) que promovem uma Internet Aberta baseada em direitos humanos, que seja Acessível a todos e caracterizada pela participaçãomultissetorial;

1.6 Fortalecer o papel transversal da Internet em todas as atividades programáticas da UNESCO, incluindo *Priority Africa, Priority Gender Equality*, apoio aos Pequenos Estados Insulares em Desenvolvimento e Países Menos Desenvolvidos, bem como na liderança da UNESCO da Década Internacional para a Reaproximação das Culturas.

2. Opções para a UNESCO relacionadas com o campo de acesso à informação e conhecimento:

2.1 Promover o acesso universal, aberto, acessível e irrestrito à informação e ao conhecimento, e diminuir a fissura digital, incluindo a disparidade de gênero, e incentivar padrões abertos, conscientizar e monitorar o progresso;

2.2 Defender políticas de TIC que melhorem o acesso guiado por princípios de governança que assegurem abertura, transparência, responsabilização, multilinguismo, inclusão, igualdade de gênero e participação civil, incluindo as relativas aos jovens, pessoas com deficiência, grupos marginalizados e vulneráveis;

2.3 Apoiar abordagens inovadoras para facilitar o envolvimento dos cidadãos em termos de desenvolvimento, implementação

e monitoramento dos Objetivos de Desenvolvimento Sustentável, conforme acordado na Assembleia Geral da ONU;

2.4 Promover o acesso universal à informação e ao conhecimento e às TICs, incentivando a criação de facilidades de acesso público, e apoiando usuários de todos os tipos para desenvolver suas capacidades de uso da Internet como criadores e usuários de informação e conhecimento;

2.5 Reafirmar a importante contribuição proporcionada pelo acesso aberto a informações acadêmicas, científicas e jornalísticas, dados governamentais abertos, e *software* livre e de código aberto, para a construção de recursos abertos de conhecimento;

2.6 Explorar o potencial da Internet para a diversidade cultural.

3. Opções para a UNESCO relacionadas ao campo da Liberdade de Expressão

3.1 Estimular os Estados-membros e outros atores a proteger, promover e implementar a legislação internacional de direitos humanos sobre livre expressão e o livre fluxo de informações e ideias na Internet;

3.2 Reafirmar que a liberdade de expressão se aplica e deve ser respeitada, *online* e *offline* em conformidade com o Artigo 19 da Declaração Universal dos Direitos Humanos e o Artigo 19 do Pacto Internacional sobre Direitos Civis e Políticos (PIDCP) que qualquer limitação à liberdade de informação deve estar em conformidade com a lei internacional de direitos humanos, de acordo com o Artigo 19 (3) do Pacto Internacional sobre Direitos Civis e Políticos;

3.3 Apoiar a segurança de jornalistas, profissionais da mídia e produtores de mídia social que geram uma quantidade significativa de material jornalístico e reafirmar a importância do Estado de direito para combater a impunidade em casos de ataques à liberdade de expressão e ao jornalismo dentro ou fora da Internet;

3.4 Observar a relevância para a Internet e as comunicações digitais da Convenção Internacional sobre os Direitos das Pessoas com Deficiência (CDPD), a Convenção sobre a Eliminação de Todas as Formas de Discriminação contra as Mulheres (CEDAW), e o trabalho do Escritório do Alto Comissário de Direitos Humanos, sobre a proibição da defesa do ódio nacional, racial ou religioso que constitui incitamento

à discriminação, hostilidade ou violência (Plano de Ação de Rabat 2012), promover mecanismos educacionais e sociais para combater o discurso de ódio *online*, sem usar os mesmos para restringir a liberdade de expressão;

3.5 Continuar o diálogo sobre o importante papel que os intermediários da Internet desempenham na promoção e proteção da liberdade de expressão;

4. Opções para a UNESCO relacionadas à Privacidade

4.1 Apoiar pesquisas para avaliar os impactos sobre a privacidade da interceptação digital, coleta, armazenamento e uso de dados, bem como de outras tendências emergentes;

4.2 Reafirmar que o direito à privacidade se aplica e deve ser respeitado *online* e *offline*, de acordo com o Artigo 12 da Declaração Universal dos Direitos Humanos e o Artigo 17 do PIDCP e no âmbito do mandato da UNESCO, os esforços relacionados à Resolução A/RES/69/166 da Assembleia Geral da ONU sobre o direito à privacidade na era digital;

4.3 Apoiar as melhores práticas e esforços empreendidos pelos Estados-membros e outras partes interessadas para abordar as questões de segurança e privacidade na Internet de acordo com suas obrigações internacionais de direitos humanos e considerar, a esse respeito, o papel fundamental desempenhado pelos agentes do setor privado;

4.4 Reconhecer o papel que o anonimato e a encriptação podem desempenhar como facilitadores da proteção da privacidade e da liberdade de expressão e facilitar o diálogo sobre essas questões.

4.5 Compartilhar as melhores práticas de coleta de informações pessoais que sejam legítimas, necessárias e proporcionais, e que minimizem os identificadores pessoais nos dados;

4.6 Apoiar iniciativas que promovam a conscientização das pessoas sobre o direito à privacidade *online* e a compreensão das formas em desenvolvimento em que governos e empresas comerciais coletam, usam, armazenam e compartilham informações, bem como as maneiras pelas quais as ferramentas de segurança digital podem ser usadas para proteger os direitos de privacidade dos usuários;

4.7 Apoiar os esforços para proteger os dados pessoais que fornecem segurança aos usuários, respeito pelos seus direitos, mecanismos de reparação e fortalecimento da confiança nos novos serviços digitais.

5. Opções para a UNESCO relacionadas com a dimensão ética da Sociedade da Informação

5.1 Promover a reflexão ética, a pesquisa e o diálogo público, com base nos direitos humanos relativos às implicações de tecnologias novas e emergentes e seus potenciais impactos sociais;

5.2 Incorporar, como um componente central em conteúdo e recursos educacionais, incluindo programas duradouros de aprendizagem, que apoiem a compreensão e a prática da reflexão ética baseada nos direitos humanos e o seu papel na vida *online* e *offline*;

5.3 Permitir que meninas e mulheres aproveitem ao máximo o potencial da Internet para a igualdade de gênero por meio de medidas proativas para remover barreiras, tanto *online* quanto *offline*, e promover sua participação igualitária;

5.4 Apoiar os formuladores de políticas na melhoria da sua capacidade de enfrentar os aspectos éticos baseados no direito humano das sociedades do conhecimento inclusivas, fornecendo treinamento e recursos relevantes;

5.5 Em reconhecimento à natureza transfronteiriça da Internet, promover a educação para a cidadania global, a cooperação regional e internacional, construção, pesquisa, intercâmbio de melhores práticas e desenvolvimento de um amplo entendimento e capacidades para responder a seus desafios éticos.

6. Opções para a UNESCO relacionadas a questões transversais:

6.1 Promover a integração da expertise da UNESCO em educação midiática e informacional em sistemas educacionais formais e informais; como reconhecimento dos importantes papéis que a educação digital e a facilitação do acesso universal à informação na Internet desempenham na promoção do direito à educação, conforme enumerado no Conselho de Direitos Humanos, Resolução 26/13;

6.2 Reconhecer a necessidade de maior proteção da confidencialidade das fontes de jornalismo na era digital;

6.3 Apoiar os Estados-membros conforme solicitado na harmonização de leis, políticas e práticas nacionais relevantes com o direito internacional dos direitos humanos;

6.4 Apoiar a transparência e a participação do público no

desenvolvimento e implementação de políticas e práticas entre todos os atores da sociedade da informação.

6.5 Promover pesquisas sobre leis, políticas, marcos regulatórios e o uso da Internet, incluindo indicadores relevantes nas áreas-chave do estudo.

6.6 Promover a participação da UNESCO nas discussões sobre Neutralidade de Rede como relevantes para os campos de acesso à informação e conhecimento e liberdade de expressão.

7. Opções relacionadas ao papel da UNESCO

7.1 Reforçar as contribuições e a liderança da UNESCO dentro do sistema da ONU, incluindo a implementação contínua dos resultados da WSIS, a revisão da WSIS+10, o IGF e a agenda de desenvolvimento pós-2015;

7.2 Envolver-se ativamente com parceiros fora do sistema da ONU, como governos individuais, sociedade civil, mídia, academia, setor privado, comunidade técnica e usuários individuais, inclusive mediante a prestação de assessoria especializada, compartilhamento de experiências, criação de fóruns para diálogos e fomento ao desenvolvimento e à capacitação dos usuários para o desenvolvimento de suas potencialidades;

7.3 Apoiar os Estados-membros na garantia de que a política e a regulamentação da Internet envolvam a participação de todas as partes interessadas e integrem direitos humanos internacionais e igualdade de gênero.

Apêndice 2: Documento conceitual da UNESCO sobre Universalidade da Internet

Universalidade da Internet: um meio para construir sociedades de conhecimento e a agenda de desenvolvimento sustentável pós-2015

2 de setembro de 2013

Resumo

O Setor de Comunicação e Informação da UNESCO busca, através de entrevistas, um novo conceito de "Universalidade da Internet", que poderia servir para destacar, de forma holística, as condições continuadas para o progresso perante a Sociedade do Conhecimento e a elaboração da Agenda de Desenvolvimento Sustentável Pós-2015. O conceito abrange, mas também supera, o acesso universal à Internet, mobilidade e TIC. A palavra "Universalidade" aponta para quatro normas fundamentais que foram incorporados na ampla evolução da Internet até hoje, e que fornecem uma maneira abrangente de entender como vários aspectos diferentes fazem parte de um todo mais amplo. Para que a Internet cumpra seu potencial histórico, ela precisa alcançar a "Universalidade" plena baseada na força e interdependência do que se segue: (i) a norma de que a Internet é baseada nos Direitos Humanos (que neste documento é o substantivo que significa "Internet livre"), (ii) a norma que é "Aberta", (iii) a norma que destaca "Acessível a Todos", e (iv) a norma que é nutrida pela participação multissetorial. As quatro normas podem ser resumidas pelo mnemônico R – O – A – M (D - A - A - M -Direitos, Abertura, Acessibilidade, Multissetorialismo). O conceito de "Universalidade da Internet" tem um valor muito específico para a UNESCO em particular. Baseando-se nas posições existentes da UNESCO na Internet, o conceito de "Universalidade da Internet" pode ajudar a estruturar grande parte do trabalho relacionado à Internet da UNESCO em Educação, Cultura, Ciências Naturais e Sociais e Informação-Comunicação para o período estratégico de 2014-2021. No que diz respeito aos debates globais sobre governança da Internet, o conceito "Universalidade da Internet" pode ajudar a UNESCO a facilitar a cooperação internacional multissetorial, bem como contribuir para destacar o que a Organização pode trazer para a Agenda de Desenvolvimento Sustentável Pós-2015.

Elaborado por: Divisão de Liberdade de Expressão e Setor de Comunicação e Informação de Desenvolvimento de Mídia[241]

* A versão integral deste documento em todas as línguas oficiais da ONU está

[241] Incorporando percepções da UNESCO Consultas intersetoriais e externas. Somos gratos também à senhora Constance Bommelaer por sua contribuição ao desenvolvimento do conceito.

disponível online em:

http://www.unesco.org/new/en/communication-and-information/crosscutting-priorities/ unesco-Internet-study/Internet-universality/

Resumo

1. Por que um conceito de "Universalidade da Internet"?

A UNESCO, há muito tempo, reconhece que a Internet tem um enorme potencial de aproximar o mundo da paz, do desenvolvimento sustentável e da erradicação da pobreza.[242] Como uma organização internacional intergovernamental que opera com um mandato global e promovendo valores que são universais, a UNESCO tem uma conexão lógica com a "universalidade" da Internet. Essa "universalidade" pode ser entendida como o fio condutor que percorre quatro dimensões sociais fundamentais referentes à Internet, ou seja, até que ponto esta facilidade baseia-se em normas universais de serem: (i) baseadas em direitos humanos (e, portanto, livres);
(ii) abertas; (iii) acessíveis a todos; e (iv) organizadas de forma a contar com a participação multissetorial. As quatro normas podem ser resumidas pelo mnemônico R-O-A-M (D - A - A - M -Direitos, Abertura, Acessibilidade, Multissetorialismo).

As múltiplas partes interessadas caracterizaram a Internet de acordo com o que percebem como suas características essenciais, destacando um aspecto ou outro, como liberdade de expressão, arquitetura aberta, questões de segurança, ética *online* etc.[243] O que esta gama de conceitualizações ilustra é tanto a diversidade das questões e interesses, como o caráter multifacetado da própria Internet. Por sua vez, isso levanta a questão sobre a possibilidade de entender como as várias considerações e dimensões se relacionam entre si e com o todo. Como um método utilizado para conceituar esse quadro maior, a UNESCO está agora analisando o conceito de "Universalidade da Internet", que poderia servir como um macroconceito. O objetivo é capturar os elementos essenciais duradouros da Internet vasta, complexa e em evolução, e que facilita uma compreensão abrangente de onde e como diferentes partes, e especialmente a UNESCO, se relacionam com a Internet. O conceito poderia particularmente servir como uma perspectiva capacitadora no contexto da crescente centralidade da Internet para as sociedades, e especificamente a crescente "Internetização" da educação, das ciências, cultura e informações relacionadas à comunicação.

Além de identificar quatro normas distintas que têm especial interesse para a UNESCO, o conceito de "Universalidade da Internet" agrupa estes sob um único cabeçalho integrado de uma maneira que permita o reconhecimento de seu caráter mutuamente reforçador e interdependente. Sem um dispositivo intelectual tão

242 Por exemplo: "Reflexão e Análise pela UNESCO na Internet: UNESCO e o uso da Internet em seus domínios de competência" (2011). http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/ED/ICT/pdf/useInternetdomains.pdf.

243 Por exemplo, houve ênfases diferentes no Fórum de Estocolmo, a *Freedom Online Coalition on Cyberspace*, Wilton Park e as conferências de Londres e Budapeste sobre o ciberespaço. Da mesma forma, a Internet foi analisada de forma diversa por organizações internacionais. Eis alguns exemplos: a Recomendação do CM da Europa CM/Rec (2011) 8 do Comitê de Ministros aos Estados membros sobre a proteção e promoção da universalidade, integridade e abertura da Internet "(2011), a Recomendação do Conselho da OCDE sobre os Princípios para a Criação de Políticas da Internet (2011), o representante da OSCE sobre a Liberdade das Recomendações de Mídia da Conferência Internet 2013 (2013); a Declaração de Política da ICC sobre "A liberdade de expressão e o livre fluxo de informações na Internet", e a Carta de Direitos e Princípios da Internet da Coalizão de Direitos e Princípios da Internet (2010).

abrangente, seria difícil entender as interconexões entre o trabalho relacionado à Internet da UNESCO e como ele contribui para as Sociedades do Conhecimento e a Agenda de Desenvolvimento Sustentável Pós-2015.

No que diz respeito ao envolvimento da UNESCO nos debates globais, o conceito de "Universalidade da Internet" pode ser considerado pelo seu potencial como um quadro unificador, consolidado e abrangente. Por um lado, destaca os princípios da liberdade e dos direitos humanos como compartilhados pelas noções existentes, como "liberdade na Internet". Por outro lado, também fornece uma cobertura para responder às questões interligadas de acesso e uso, assim como questões de abertura técnica e econômica. Além disso, o conceito também engloba o envolvimento de diversas partes interessadas como um componente integral. Desta forma inclusiva, o conceito "Universalidade da Internet" pode, portanto, ser uma estrutura de ponte e visão de futuro para o diálogo entre o Norte e o Sul e entre as diferentes partes interessadas. Como tal, poderia também dar uma contribuição única para moldar o discurso global sobre governança da Internet e a Agenda de Desenvolvimento Sustentável pós-2015.

2. Elucidando o conceito de "Universalidade da Internet"

O vínculo entre quatro componentes normativos da "universalidade" da Internet está intimamente ligado ao conceito anterior da UNESCO sobre a Internet, que contempla:

- *Recomendação sobre a Promoção e Utilização do Multilinguismo e Acesso Universal ao Ciberespaço* (2003).[244] (Este documento aponta particularmente para a norma de acessibilidade, bem como para a necessidade de harmonizar os direitos).

- *Reflexão e Análise da UNESCO na Internet* (2011).[245] (Este documento destaca o trabalho normativo em relação aos programas da UNESCO e a participação de diversas partes interessadas).

- *Recomendações Finais do evento de revisão da WSIS+10*, e a *Declaração Final do evento de revisão da WSIS+10* (2013).[246] (Estes contemplam direitos, acesso, abertura e questões multissetoriais).

- *UNGIS (UNGrouponthe Information Society) Declaração Conjunta sobre a Agenda de Desenvolvimento Sustentável Pós-2015* (2013).[247] (Este documento destaca a importância das condições sociais para as

244 http://www.unesco.org/new/en/communication-and-information/about-us/how-we-work/strategy-and-programme/promotion-and-use-of-multilingualism-and-universal-access-to-cyberspace/.

245 http://unesdoc.unesco.org/images/0019/001920/192096e.pdf;

246 Documents from the First WSIS+10 Review Event, "Towards Knowledge Societies for Peace and Sustainable Development", Paris 25-27 February, 2013: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/wsis/WSIS_10_Event/wsis10_recommendations_en.pdf; http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/wsis/WSIS_10_Event/wsis10_final_statement_en.pdf

247 http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/wsis/ungis_joint_statement_wsis_2013.pdf.

> Tecnologias da Informação e Comunicação em geral, e a Internet, em particular, de forma a contribuir com as Sociedades do Conhecimento inclusivas).

A "Universalidade da Internet" integra uma variedade de percepções existentes da UNESCO e apresenta a relação entre a Internet e o que a UNESCO já reconheceu[248] como os princípios fundamentais subjacentes das Sociedades do Conhecimento: liberdade de expressão, educação de qualidade para todos, acesso universal à informação e ao conhecimento e respeito à diversidade cultural e linguística. Desta forma, o conceito destaca o que é necessário para que a Internet seja um meio para alcançar as Sociedades do Conhecimento. Atuando esta como uma heurística para destacar que o caráter e a utilidade da Internet envolvem mecanismos técnicos, sociais, legais, econômicos e outros, que, por sua vez, dependem de normas particulares que sustentam a potencialidade positiva desses instrumentos. Consideradas com mais profundidade, as normas R-O-A-M (D - A - A – M) constitutivas da "Universalidade da Internet" (Direitos, Abertura, Acessibilidade, Multissetorialismo) podem ser entendidas da seguinte forma:

(i) Ao se identificar a conexão da Internet com as normas baseadas nos Direitos Humanos como constituintes da liberdade, A "Universalidade da Internet" ajuda a enfatizar a harmonia contínua entre o crescimento e uso da Internet e dos direitos humanos. Uma Internet livre, nesse sentido, significa respeitar e possibilitar a liberdade de exercer os direitos humanos.[249] A este respeito, "Universalidade da Internet" nos conduz a considerar a gama de interdependências e inter-relacionamentos entre diferentes direitos humanos e a Internet – tais como liberdade de expressão, privacidade, participação cultural, igualdade de gênero, associação, segurança, educação, etc.

(ii) A "Universalidade da Internet" também destaca a norma da Internet ser aberta. Esta designação reconhece a importância de questões tecnológicas como padrões abertos, bem como padrões de acesso aberto ao conhecimento e à informação. A abertura também sinaliza a importância da facilidade de entrada de atores e a ausência de fechamento que poderia ser imposto pelos monopólios.

(iii) Acessível a Todos como norma da "Universalidade da Internet" levanta questões de acesso e disponibilidade técnica, além de divisões digitais, baseadas em renda econômica e desigualdades urbano-rurais. Assim, aponta para a importância de normas em torno do acesso universal a níveis mínimos de infraestrutura de conectividade. Ao mesmo tempo, "acessibilidade" requer o envolvimento com exclusões sociais da Internet com base em fatores como educação, linguagem, classe, gênero e deficiência. Além disso, entender que as pessoas acessam a Internet como produtoras de conteúdo, código e aplicativos, e não apenas como consumidores de informação e serviços. A

---

248 *Reflection and Analysis by UNESCO on the Internet,* http://unesdoc.unesco.org/. images/0019/001920/192096e.pdf.

249 Desta forma, "Universalidade da Internet" está de acordo com o Relatório do Relator Especial da ONU sobre a promoção e proteção do direito de liberdade de opinião e expressão e também faz eco da primeira resolução sobre "promoção, proteção e exercício dos direitos humanos na Internet ", aprovada pelo Conselho de Direitos Humanos da ONU em 2012.

questão das competências dos usuários é parte da dimensão de acessibilidade da "Universalidade". Isto destaca a noção da UNESCO de Educação de Mídia e Informação que melhora a acessibilidade, capacitando os usuários da Internet a se engajarem de maneira crítica, competente e ética.

(iv) A Internet, nesse sentido, não pode ser vista apenas do "lado do fornecedor", mas precisa de uma perspectiva complementar "centrada no usuário". A dimensão participativa, e especificamente a participação multissetorial da "Universalidade da Internet" facilita a criação de sentido das funções que agentes diferentes (representando diferentes setores, assim como diferentes status social e econômico, e não excluindo mulheres e meninas) têm desempenhado, e precisam continuar a jogar, desenvolvendo e governando a Internet em vários níveis. A participação é essencial para o valor que a instalação pode ter para a paz, o desenvolvimento sustentável e a erradicação da pobreza. Ao unir os interesses das partes interessadas, os mecanismos participativos contribuem para normas compartilhadas que atenuam os abusos da Internet. A "universalidade", nesse caso, destaca a governança compartilhada da Internet.

Tais normas para estes quatro aspectos são distintas, mas também reforçam umas às outras. Direitos sem acessibilidade seriam limitados a poucos; acessibilidade sem direitos prejudicaria o potencial de acesso. A abertura permite o compartilhamento e a inovação e complementa o respeito pelos direitos e acessibilidade. A participação de vários interessados ajuda a garantir as outras três normas. Em geral, uma Internet que falha em respeitar os direitos humanos, a abertura, acessibilidade ou participação de várias partes interessadas estaria, por definição, muito aquém de ser considerada universal.

3. Como o conceito de "Universalidade da Internet" é relevante para a UNESCO

A UNESCO tem o papel único de promover a "Universalidade da Internet". É a agência da ONU com um mandato que abrange a vida social em geral e, nesse âmbito, possui programas que envolvem a Internet na educação, cultura, ciência, ciências sociais e informações relacionadas à comunicação. Ao usar a "Universalidade da Internet" como um conceito abrangente, a UNESCO pode posicionar preocupações mais específicas, como a aprendizagem móvel, educação para meninas, diversidade cultural e linguística, educação midiática e informacional, pesquisa sobre as alterações climáticas, liberdade de expressão, acesso universal à informação, bioética e inclusão social, etc. Dessa forma, a "Universalidade da Internet" também pode apoiar as prioridades relacionadas à igualdade de gênero e à África. Pode servir como uma estrutura abrangente e integradora para o trabalho relacionado à Internet em toda a UNESCO, estabelecendo um quadro comum de referência para todos. Operacionalmente, o conceito pode elevar uma série de trabalhos ao status de iniciativas que promovem em conjunto a "Universalidade da Internet". Pode incentivar sinergias e cooperação intersetorial e programação conjunta. Em particular, o conceito pode melhorar a compreensão da estratégia de médio prazo de 2014-2021 (37/C4) e do programa quadrienal (37/C5).

4. Conclusão

A “Universalidade da Internet” está de acordo com o serviço da Organização para a comunidade internacional em geral nos seguintes aspectos:

- Laboratório de ideias, incluindo a previsão - a elaboração do conceito é diretamente relevante para o potencial criativo e o *think-tank* da UNESCO;
- Ao estimular o debate global, a “Universalidade da Internet” ilustra como a UNESCO pode ser um catalisador para a cooperação internacional, com uma abordagem holística e inclusiva;
- Definir padrões – se o conceito ganhou força de forma ampla, poderia informar o desenvolvimento de padrões para monitorar o progresso na “Universalidade da Internet”;
- Como um quadro normativo que pode informar as políticas, e atrair público e privado, sociedade civil e tomadores de decisão, a “Universalidade da Internet”, pode ajudar a UNESCO a cumprir seu papel de construtor de capacidades nos Estados-membros.

Olhando para o futuro, a “Universalidade da Internet” poderia seguir os passos dos influentes trabalhos intelectuais anteriores da UNESCO como os conceitos de “Patrimônio Cultural Imaterial” e “Sociedades do Conhecimento”. Tendo em vista que a “Universalidade da Internet” representa uma conceituação atualizada da época, o conceito pode se tornar uma contribuição valiosa para a discussão global sobre essa criação humana complexa e dinâmica e serve para melhorar a contribuição contínua da Internet para o futuro compartilhado da humanidade.

Direitos Humanos e Criptografia

Esta publicação segue a nova abordagem da UNESCO para as questões da Internet, conforme endossada em novembro de 2015, por ocasião de sua 38ª Conferência Geral. Os nossos 195 Estados-membros adotaram o Documento Final "*Connecting the Dots"* em que 38 opções de ações futuras da UNESCO são estabelecidas; e os princípios da Universalidade da Internet (ROAM), que defendem uma Internet aberta e acessível baseada em direitos humanos, regida pela participação de múltiplas partes interessadas.

A criptografia é um tema importante na atual discussão global sobre governança da Internet. A presente pesquisa se debruça sobre o assunto e busca delinear uma visão global dos vários meios de encriptação, sua disponibilidade e suas possíveis aplicações no cenário de mídia e comunicações. A pesquisa explica como a implementação da encriptação é afetada por diferentes áreas do direito e da política, bem como oferece estudos de caso detalhados de encriptação em jurisdições selecionadas.

Analisa em profundidade o papel da encriptação no cenário de mídia e comunicações e o impacto em diferentes serviços, entidades e usuários finais. Com base nessa exploração e análise, a pesquisa fornece recomendações sobre políticas de encriptação que são úteis para várias partes interessadas, as quais incluem sinalizar a necessidade de combater a falta de igualdade de gênero no debate atual e também destacar ideias para melhorar a "alfabetização criptográfica".

UNESCO
Organização das Nações Unidas para a Educação, Ciência e Cultura

Setor de Comunicação e Informação

9 789231 001857