Nota Técnica da Sociedade Civil para a CPI de Crimes Cibernéticos

Coding Rights e Instituto Beta para Internet e a Democracia

04/04/2016

Sumário

1 Sumário Executivo **3**
- 1.1 Manutenção da neutralidade da rede, liberdade de expressão e do regime de responsabilidade limitada de Intermediários já previstos no Marco Civil 3
- 1.2 Não criminalização de tecnologias de segurança e anonimato como medida de segurança 4
- 1.3 Perigos da aplicação de um conceito vago de segurança cibernética 5
- 1.4 Importância de um debate multissetorial para tratar de crimes cibernéticos . . . 6
- 1.5 Considerações finais 6

2 Introdução **8**
- 2.1 CPI de Crimes Cibernéticos 8

3 Crime Cibernético **11**

4 Marco Civil da Internet **13**
- 4.1 Regulamentação do Marco Civil da Internet 15

5 Retenção de Registros de Conexão e Aplicações **18**
- 5.1 Marco Civil da Internet 18
- 5.2 Violação de direitos? 18
- 5.3 Custos 20
- 5.4 Vazamentos 20
- 5.5 Metadados 21
- 5.6 Retenção mínima 23

6 Criptografia **25**
- 6.1 Ubíqua e vital 26
- 6.2 Sem porta dos fundos 29
- 6.3 Chaves debaixo do carpete 29
- 6.4 Um exemplo vivo: Juniper e o backdoor do backdoor 30

7 Interceptação **31**
- 7.1 Panorama Legal 31

7.2 Comunicações em trânsito vs. comunicações armazenadas 33

8 Anonimato Online **37**
8.1 Vedação constitucional 37
8.2 Usos legais do anonimato no Brasil 38
8.3 Espaços anônimos e espaços vigiados 40
8.4 ONU: proteção à privacidade, à criptografia e ao anonimato 47
8.5 Anonimato é legião, porque são muitos 48
8.6 Por uma reinterpretação do anonimato 50

9 Tor e Rede Onion **52**
9.1 Tor 52
9.2 Rede Onion e Onion Web 56
9.3 Quebras da Rede Onion em investigações policiais 58

10 Segurança Cibernética **61**
10.1 Definição 61
10.2 Brasil 62
10.3 Cenário internacional 67

11 Questões Emergentes **76**
11.1 Deep Web 76
11.2 Pornografia Infantil 78
11.3 Invasão de computadores 81

12 Créditos **87**
12.1 Redação 87
12.2 Apoio 88
12.3 Agradecimentos 88

13 Referências **89**

14 Propostas para o Relatório Final da CPICIBER **90**
14.1 Apresentação 90
14.2 Proposta nº 1: Substituir conceitos erroneamente definidos ou irrelevantes . . . 91
14.3 Proposta nº 2: Redação mais precisa no Art. 154-A do Código Penal 92
14.4 Proposta nº 3: Substituir utilização do Fistel pela utilização do FNSP 94
14.5 Proposta nº 4: Regras para indisponibilização de conteúdo infringente idêntico . 97
14.6 Proposta nº 5: Não permitir o acesso ao endereço IP sem ordem judicial 100
14.7 Proposta nº 6: Não permitir bloqueio de aplicações 101
14.8 Proposta nº 7: Não ampliar o acesso ao cadastro de usuários de telefones pré-pagos 102
14.9 Proposta nº 8: Não indicar à ANATEL a adoção do IPv6 104
14.10 Proposta nº 9: Não endossar a ampliação da guarda de registros de conexão . . 105
14.11 Considerações finais 107

CAPÍTULO 1

Sumário Executivo

Este documento visa oferecer insumos à CPICIBER, tendo em conta o desafio de viabilizar o **combate aos cibercrimes** de maneira equilibrada com a **proteção de direitos fundamentais**. Contudo é com preocupação que as organizações da sociedade civil que assinam este documento recebem o relatório final desta CPI.

É importante **evitar que, sob a égide da segurança, o próprio Estado incorra em violações** sistemáticas de direitos fundamentais de milhões de indivíduos que usam tecnologias da informação e comunicação (TICs) para práticas cotidianas e essenciais ao exercício da democracia. Para tal, viemos por meio desta prover mais **informações técnicas** tanto sobre o funcionamento da rede, bem como **ressaltar de direito e deveres** já estabelecidos no que diz respeito aos usos da Internet no Brasil, para que se reavalie algumas proposições do relatório final.

O combate ao cibercrime, cometido via ou com a ajuda de TICs, deve acatar aos limites legais estabelecidos na Constituição Federal, bem como em outras normas específicas, especialmente o Marco Civil da Internet, lei aprovada no Congresso Nacional em 2014, que, entre outros direitos, prevê garantias como **a liberdade de expressão, o sigilo de comunicações, presunção de inocência, privacidade e proteção de dados pessoais no âmbito da Internet**. Ressalta-se que o **Marco Civil da Internet é produto de um longo processo de consultas públicas e diálogo** entre os diversos setores interessados, portanto, produto de um consenso sedimentado depois de longo diálogo. **Consideramos precipitadas sugestões de alterações deste texto de lei**, ainda mais quando se altera todo o balanço que se obteve após anos de negociação, **principalmente no que diz respeito à responsabilidade de intermediários por conteúdo de terceiros, neutralidade de rede e proteção da privacidade**, com todas as salvaguardas estabelecidas por termos estabelecido um regime de guarda obrigatória de registros.

1.1 Manutenção da neutralidade da rede, liberdade de expressão e do regime de responsabilidade limitada de Intermediários já previstos no Marco Civil

Acreditamos que **a neutralidade de rede deve ser garantida, sem exceções**, a não ser aquelas previstas no próprio Marco Civil da Internet e em sua vindoura regulamentação **[#f1]_**. Legitimar o bloqueio de aplicações no nível dos provedores de conexão obriga tais provedores a

manter **listas negras** de endereços IP, atualizadas e fiscalizadas pelas autoridades competentes, a semelhança do que ocorre com a muralha virtual da China, para assim impedir pacotes de chegar até tais endereços. Trata-se, mais uma vez, de clara **contradição ao Marco Civil da Internet**, que estabelece em seu art. 9º que "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".

Também vemos com preocupação surgirem **propostas de procedimentos específicos para a remoção de determinados tipos de conteúdo**. Lembramos também que encumbir provedores e serviços de **monitorar e remover cópias de um conteúdo** de suas plataformas através de similaridade e não de links ou URL's específicos pode ser **tecnicamente custoso e desafiador**, devendo qualquer ordem judicial nesse sentido ser **determinar conteúdos específicos**, sendo que a aplicação em si não deveria ser alvo de bloqueios, sob pena de restringir o acesso a conteúdo e a liberdade de expressão.

No que tange o balanço hoje estabelecido para a proteção de dados dos usuários da rede, para qualquer proposta normativa que vise combater cibercrimes, as previsões de **retenção e acesso a esses dados**, inclusive metadados, devem ser **excepcionais e mínimas**, devendo respeitar o princípio da presunção de inocência, pois, caso contrário, prejudica-se a privacidade das comunicações e constrange-se o exercício da **liberdade de expressão e associação**; além de se criar um alto custo de operação e segurança de centros de dados e ampliar o **risco de acesso não autorizado e de vazamentos**, trazendo, assim, mais insegurança.

Nesse contexto, o **Marco Civil da Internet já definiu o que são dados cadastrais** no contexto da provisão de serviços da rede e **já estabeleceu que número de IP não se inclui nesta definição, mas sim na definição de registros de conexão e aplicações**, que tem regimes próprios para guarda e acesso. Novamente, desconsiderar todos os anos de debate multissetorial que se teve para chegar a este regime seria uma afronta ao processo democrático do Marco Civil.

Alterações não deveriam vir para mudar completamente a essência do que se tem hoje acordado, mas sim para melhorar sua aplicação. Nesse sentido, por exemplo, **parâmetros protetivos e de transparência**, presentes na Lei de Interceptação Telefônica, na Lei Geral de Telecomunicações e no Marco Civil da Internet, poderiam ser aprimorados para **assegurar a proteção de direitos e a integralidade dos sistemas de tecnologias de informação e comunicação**, de modo que seja sempre possível a supervisão e revisão judicial das atividades da Polícia e do Ministério Público, e até mesmo do próprio Poder Judiciário.

1.2 Não criminalização de tecnologias de segurança e anonimato como medida de segurança

Além do respeito ao ambiente jurídico de proteção de direitos na rede, entende-se que o reconhecimento da **legitimidade de tecnologias de proteção e segurança**, como a **criptografia**, são necessários para assegurar a confidencialidade, autenticidade e integridade nas comunicações realizadas entre pessoas e empresas, ou mesmo no âmbito do Poder Público. A **criminalização** e a imposição de quaisquer **fraquezas de chaves e algoritmos**, mesmo para combater ilícitos, abririam **portas dos fundos para criminosos e nações mal intencionadas** poderem atacar justamente aqueles inocentes que o Estado pretende defender dos cibercrimes.

Outro ponto crucial é, sem afronta à vedação constitucional, **não confundir o anonimato, por si só, com a efetiva prática de um crime**. Cabe lembrar que **a proteção da identidade é prevista em lei**, sendo a **base para viabilizar denúncias anônimas**, o sigilo de **fonte jornalística**, e outras manifestações do pensamento em contextos em que a transmissão de informação pode prejudicar a integridade física do interlocutor.

Sugere-se expressamente o entendimento e consideração de que o **anonimato também pode ser utilizado como via de exercício do direito de acesso à informação**, virtual ou presencial, sem ser identificado ou enquadrado em determinado perfil que possa ser alvo de discriminações. Igualmente, faz-se necessária a discussão sobre como práticas para **proteger a identidade** também podem servir como **mecanismo de segurança** ao debater opiniões de dissenso em ambiente seguro, contra eventuais ataques arbitrários e ilegais, como no caso de questões **pertinentes a diversos tipos de minorias** que são alvos destes ataques, inclusive em ambientes tão democráticos quanto o Brasil.

A conhecida **tecnologia Tor** viabiliza uma rede que funciona impedindo que tanto o provedor de conexão quanto o servidor de aplicações online possam ligar os pacotes de dados ao endereço IP de quem os acessou. Além de servir de ferramenta de evasão da censura, viabilizando o acesso a sites bloqueados em países mais autoritários (por exemplo, o uso de redes sociais na China e na Turquia), essa ferramenta também é usada por veículos da grande imprensa (Washington Post, Guardian, New Yorker, Forbes) e por ONGs, como **instrumento essencial para operar em pautas que vão desde o combate do contrabando de animais até denúncias de corrupção**. No interesse do Poder Público, muitos países se valem do Tor inclusive em **investigações policiais**. Portanto, devem ser **incentivadas técnicas de investigação que não se oponham à natureza descentralizada desta rede**, pois qualquer quebra, invasão ou censura particular comprometeriam sua totalidade da mesma. Não se podem confundir tecnologias com eventuais **condutas ilícitas adotadas mediante o seu uso**.

Neste mesmo contexto, vemos com preocupação a criação e a ampliação de **mecanismos de identificação de acesso** à Internet e à telefonia móvel. Nas palavras do Relator para a promoção e proteção do direito à liberdade de expressão e opinião da ONU, obrigações como a de **vincular identificações à cartões SIM** "podem providenciar a Governos a **capacidade de monitorar indivíduos e jornalistas além de qualquer interesse legítimo**", e "a possibilidade de um Estado **obrigar provedores de conexão e aplicação a coletar e armazenar registros** documentando as atividades online de todos os seus usuários inevitavelmente resultou em um **Estado que possui os rastros digitais de todas as pessoas**".

1.3 Perigos da aplicação de um conceito vago de segurança cibernética

Também é importante ver criticamente o **conceito de "segurança cibernética", cujo significado, carente de padrão ou consenso internacional**, pode abranger distintos problemas e inconvenientes, bem como ensejar falsas soluções técnicas e legislativas deletérias que envolvem desde monitoramento excessivo até censura e perseguição. Sugere-se considerar práticas específicas ao invés de se adotar um termo tão abrangente que se esvai em si. Considerações mais específicas também tendem à levar ao entendimento de que parte de condutas que aparentam ser distintas apenas por ocorrerem no meio virtual, na realidade já têm respaldo na

legislação em vigor. Enquanto que conceitos amplos podem levar até mesmo à criminalização de condutas cotidianas de usuários comuns, como é o caso da proposta de projeto de lei que trata de invasões de sistemas e que pode vir a criminalizar condutas comum e correntes que simplesmente vão contra os termos de usos de plataformas. Termos de usos que, por sua vez, muitas vezes nem são coerentes com a legislação nacional.

1.4 Importância de um debate multissetorial para tratar de crimes cibernéticos

Por fim, uma estratégia nacional ou pactos multilaterais internacionais sobre o tema devem priorizar **processos de deliberação de que participem tanto governos quanto empresas, sociedade civil, academia e outros segmentos sociais. Caso contrário**, o debate é focado apenas em crime e terrorismo cibernéticos, por uma **perspectiva precipitada e estritamente penal e militar da discussão de segurança pública, em detrimento de outros direitos.**

Destaca-se que, a exemplo do Comitê Gestor da Internet, das consultas públicas do Marco Civil até à realização do evento diplomático internacional NetMundial, o Brasil tem sido pioneiro no incentivo a uma **estratégia de discussão multissetorial** dos temas que dizem respeito aos direitos e deveres no uso da Internet. Tal pioneirismo deve se expandir também para promover uma discussão balanceada sobre cibercrimes e cibersegurança, bem como uma clara definição específica de seus significados.

1.5 Considerações finais

Para maiores informações sobre cada um dos conceitos e argumentos ora apresentados, formulou-se uma **Nota Técnica, detalhada e ilustrada**, disponível integralmente no endereço https://cpiciber.codingrights.org. A nota traz discussões de conceitos chave para o desenvolvimento dos debates na CPICIBER, sob a ótica da análise jurídica e do funcionamento das tecnologias em questão.

Ademais, seguimos à disposição para quaisquer futuras eventualidades no encerramento dos trabalhos desta Comissão, bem no debate de propostas normativas relacionadas.

Brasília, 4 de abril de 2016.

- Lucas Teixeira, Diretor Técnico e Joana Varon, Diretora Geral – **Coding Rights**
- Paulo Rená da Silva Santarém, chefe executivo de pesquisa – **IBIDEM - Instituto Beta para Internet e Democracia**

Subscrevem esta nota técnica:

- Arpub – Associação Brasileira de Rádios Públicas
- Associação Nacional de Pós-graduação e Pesquisa em Educação – ANPEd
- Associação Software Livre.Org

- Casa da Cultura Digital Porto Alegre
- Centro de Estudos da Mídia Alternativa Barão de Itararé
- Centro de Produção, Promoção e Formação em Arte e Cultura/ArtEstação
- Centro de Tecnologia e Sociedade da FGV do Rio de Janeiro
- Ciranda Internacional da Comunicação Compartilhada
- Coding Rights
- Coletivo Digital
- FNDC – Fórum Nacional pela Democratização da Comunicação
- Geledes - Instituto da Mulher Negra
- IDEC – Instituto Brasileiro de Defesa do Consumidor
- Instituto Bem Estar Brasil
- Instituto Brasileiro de Políticas Digitais – Mutirão
- Internet Sem Fronteiras – Brasil
- Intervozes – Coletivo Brasil de Comunicação Social
- Movimento Mega
- Projeto Saúde & Alegria, Santarém, Pará
- PROTESTE - Associação de Consumidores
- #RedeLivre
- SBPC – Sociedade Brasileira para o Progresso da Ciência
- ULEPICC-Br – União Latina de Economia Política da Informação, da Comunicação e da Cultura - Capítulo Brasil

CAPÍTULO 2

Introdução

As organizações da sociedade civil têm acompanhado com preocupação as sessões da Comissão Parlamentar de Inquérito de Crimes Cibernético - CPICIBER. O volume de informações e a diversidade de visões podem confundir os parlamentares e induzir a erros no momento de compreender qual a melhor legislação a ser proposta. Como forma de organizar nossa colaboração, apresentamos aqui os principais conceitos já fixados em lei, bem como os pontos em disputa.

2.1 CPI de Crimes Cibernéticos

A CPI de Crimes Cibernéticos (CPICIBER) foi criada em agosto de 2015, em atendimento ao requerimento apresentado em fevereiro de 2015 pelo Deputado Sibá Machado (PT/AC), apoiado por outros 195 deputados.

Na proposta inicial, além de enumerar diversos exemplos, três fatos foram destacados como justificativas: (i) a Polícia Federal realizou em 2014 a operação batizada de IB2K para desarticular uma quadrilha suspeita de desviar pela Internet mais de R$ 2 milhões de correntistas de vários bancos, parte para comprar armas e drogas; (ii) o relatório da Central Nacional de Denúncias de Crimes Cibernéticos apontou crescimento, entre 2013 e 2014, de 192,93% nas denúncias envolvendo páginas na Internet suspeitas de tráfico de pessoas, e (iii) o gasto, informado pela Symantec, de US$ 15,3 bilhões com crimes cibernéticos no Brasil em 2010.

Na proposta inicial, além de enumerar diversos exemplos, três fatos foram destacados como justificativas: (i) a Polícia Federal realizou em 2014 a operação batizada de IB2K para desarticular uma quadrilha suspeita de desviar pela Internet mais de R$ 2 milhões de correntistas de vários bancos, parte para comprar armas e drogas; (ii) o relatório da Central Nacional de Denúncias de Crimes Cibernéticos apontou crescimento, entre 2013 e 2014, de 192,93% nas denúncias envolvendo páginas na Internet suspeitas de tráfico de pessoas, e (iii) o gasto, informado pela Symantec, de US$ 15,3 bilhões com crimes cibernéticos no Brasil em 2010.

Após dezenas de reuniões deliberativas e audiências públicas, a CPI ouviu vários setores da sociedade e discutiu uma gama de outros crimes e condutas que passam pelo uso de computadores e da Internet, como:

- Políticas de prevenção e resposta a abusos e crimes cibernéticos por empresas privadas do ramo digital como Facebook, Twitter, Google, Yahoo!, Microsoft e Whatsapp;

- Grupos e centros de resposta e tratamento de incidentes de segurança
- (CSIRT's / CERT's);
- Violência sexual contra crianças e adolescentes;
- Práticas abusivas de publicidade online direcionadas ao público infantil;
- Pornografia de revanche (revenge porn);
- Segurança digital das comunicações de órgãos do governo;
- Procedimentos e obstáculos no combate a crimes cibernéticos por delegados(as) de polícia, defensores(as) públicos(as) promotores(as) de justiça, analistas e outros(as) profissionais especializados na área;
- Criminalística e perícia forense de crimes cibernéticos;
- Operações policiais bem-sucedidas sobre crimes cibernéticos (como a
- Operação Barba Negra e a Operação Darknet);
- Defesa e segurança cibernética de infraestruturas críticas (bancos,
- indústria, telecomunicações, previdência social, Receita Rederal,
- sistema eleitoral);
- Proteção de consumidores contra monitoramento e uso abusivo de dados
- pessoais;
- Publicidade de empresas e setores do governo em sites de conteúdo
- ilícito, como streaming de vídeos em violação aos direitos autorais;
- Governança da Internet;
- Produção e disseminação de pornografia infantil, bem como abordagens
- policiais para repressão destes crimes, abordagens de educação e
- segurança para prevenção, abordagens psicológicas e sociais para
- tratamento de vítimas e abordagens jurídicas para responsabilização de
- criminosos;
- Depoimentos de vítimas de calúnia, racismo e crimes de ódio na Internet;
- Anonimato e pseudonimato em redes sociais e plataformas online
- ("perfis falsos / fake");
- Terrorismo e segurança cibernética durante os Jogos Olímpicos de 2016
- e em outros Grandes Eventos;
- Limites jurídicos e técnicos do provimento de dados de aplicação por
- empresas prestadoras de serviços digitais como Whatsapp e Google;
- Ações online em defesa dos direitos das mulheres (grupo ThinkOlga);

- Legislação dos estados americanos sobre provedores de Internet
- (diligência, na embaixada dos EUA em Brasília);
- Uso de software para enganar exames de emissão de poluentes pela
- empresa Volkswagen;
- Venda de medicamentos abortivos pela Internet;

Para organizar os resultados, foram designadas quatro sub-relatorias:

1. Instituições financeiras e comércio virtual – Sub-Relator Dep. Sandro Alex (PPS/PR)
2. Crimes contra a criança e o adolescente – Sub-Relator Dep. Rafael Motta (PROS/RN)
3. Violações a direitos fundamentais e criação de perfis falsos ou satíricos com o objetivo de praticar subtração de dados, crimes contra a honra, inclusive injúrias raciais, políticas, crimes de racismo, crimes contra homossexuais, estelionato, extorsão e outros ilícitos penais, intimidação, intimidação sistemática (bullying) e referências depreciativas repetidas a determinada pessoa – Sub-Relator Dep. Daniel Coelho (PSDB/PE); e
4. Segurança cibernética no Brasil – Sub-Relator Dep. Rodrigo Martins (PSB/PI)

No site da CPICIBER na Câmara dos Deputados é possível ver o histórico de reuniões passadas e assistir gravações de áudio e vídeo das sessões.

É de se preocupar o fato de que o volume e diversidade dos temas em questão – cujo debate demanda tanto um conhecimento extensivo sobre o funcionamento de diversas tecnologías, bem como o aprofundamento de discussões jurídicas ainda não pacíficas no Brasil e no mundo – possa confundir os parlamentares e induzir a erros no momento de compreender qual a melhor legislação a ser proposta.

Desta maneira, a Coding Rights, em parceria com o Ibidem, como organizações com fins sociais que seguem os debates sobre a proteção dos direitos na rede, pretendendo auxiliar no trabalho desta comissão, pretendem por meio desta estudo destacar e esclarecer o que consideramos ser os principais conceitos pertinentes aos debates que se desencadearam nas audiências públicas, trazendo tanto clareza técnica quanto a perspectiva da proteção de direitos para quando se trata de segurança no ambiente virtual.

A Coding Rights é uma organização brasileira, criada e liderada por mulheres, com sede no Rio e em São Paulo. Dedica-se a promover a integração do entendimento e uso da tecnologia nos processos de construção de políticas públicas para avançar na garantia dos direitos humanos no mundo digital.

Contatos:

- Joana Varon, Diretora Fundadora <joana@codingrights.org> e
- Lucas Teixeira, Chief Technologist <lucas@codingrights.org>

O IBIDEM – Instituto Beta para Internet e Democracia é uma associação sem fins lucrativos, baseada em Brasília, que atua na defesa e promoção de direitos humanos no ambiente digital.

Contatos:

- Paulo Renná <paulo@ibidem.org.br>

CAPÍTULO 3

Crime Cibernético

O uso criminoso de tecnologias de informação e comunicação tem sido discutido, inclusive no âmbito internacional, sempre com a necessidade de se equilibrar a proteção de direitos fundamentais. Já em 1990 o Oitavo Congresso das Nações Unidas para a Prevenção de Crime adotou uma resolução sobre "crimes relacionados ao uso de computadores" (*computer-related crimes*). Uns anos mais adiante, em novembro de 2000, o Terceiro Comitê (Comitê Social, Humanitário e Cultural) da Assembléia Geral da ONU, como parte de seu trabalho na prevenção de crimes e justiça criminal, discutiu uma resolução A/55/59 entitulada "Combate ao uso criminoso de tecnologias da informação" (*Combating the criminal misuse of information technologies*), o texto foi adotado na Assembléia Geral da ONU em 2001 e ressalta que "a luta contra o uso criminoso das tecnologiea de informação requer o desenvolvimento de soluções que levem em conta tanto a proteção de liberdades individuais e a privacidade e a preservação da capacidade de governos para lutar contra tal mal uso criminal." *[UNGA-CRIMINAL-2001]* (Página 113)

Nesse **contexto da discussão internacional**, ressaltou-se, portanto, não só a noção de que se **deve haver um balanço entre as práticas de combate a esse tipo de práticas com a proteção do direito à privacidade** e outras liberdades, **mas também a idéia de que o uso criminoso é um "mal uso" dessas tecnologias, ou seja, não é a existência dessas tecnologias em si que deve ser o foco das ações de combate a delitos**. Essa mesma noção perpassou a nova versão dessa resolução, aprovada em 2002, também pela Assembléia Geral.

A partir daí a discussão dessas práticas no sistema ONU tomou mais corpo no âmbito da Comissão para a Prevenção de Crimes e Justiça Criminal. Até então o termo "ciber" ou "cyber" não havia sido mencionado para tratar de questões de ordem criminal, apenas em um contexto militar, de segurança do Estado, no contexto do Segundo Comitê da Assembléia Geral (Comitê Econômico e Financeiro), que em 2002 discutia uma resoluções sobre uma "cultura global de cibersegurança". De acordo com Tim Maurer, o primeiro registro que se tem para uma Convenção das Nações Unidas contra o crime cibernético aparece nos relatórios de 2004 desta Comissão. Ainda assim, de acordo com o esboço de resolução que foi proposto neste mesmo relatório para a ECOSOC (entitulado "International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes"), entendia-se o escopo dessas práticas como algo delineado para tratar de fraudes e crimes de falsificação de identidade. De 2008 em diante, a mesma Comissão integra os conceitos de "fraude econômica" e "crime de identidade" nas suas sessões temáticas e esboços de resoluções para tratar de crimes cibernéticos, sendo que em 2010, o escopo se expande também para tratar da "proteção de crianças na era digital: o mal uso das tecnologias no abuso e exploração de crianças." Novamente, a idéia de "mal uso" das tecnologias encontrava-se

na terminologia. Mais adiante, e já sob a terminologia de crime cibernético (*cybercrime*), o Escritório das Nações Unidas sobre Drogas e Crime também passou a realizar estudos sobre o tema no escopo de suas atividades, o mesmo ocorrendo outras agências do sistema ONU, como a União Internacional de Telecomunicações, a UNESCO, entre outras, cada uma, teoricamente, tratando do mal uso das TICs nos temas de suas competências, como segurança da infraestrutura das redes de telecomunicações; educação e diversidade cultural, etc.

Essa tendência nos fóruns multilaterais, bem como a diversidades de temas abordados na dezena de audiências públicas realizadas no âmbito desta CPI de Crimes Cibernéticos, denota que tal conceito vem sido gradualmente utilizado para abranger uma maior diversidade de condutas online. Entretanto, antes de tudo, deve-se atentar para o fato de que um termo genérico para abranger condutas criminais específicas, na maioria das vezes muito distintas e com consequências diversas, tende a causar mais confusão do que soluções, uma vez que o conceito se dilui em múltiplas frentes e pode ensejar falsas soluções legislativas que, generalizadas, podem resultar em práticas que vão desde o monitoramento excessivo até censura e perseguição de vozes dissidentes. Sugere-se, portanto, considerar práticas específicas para adotar soluções específicas compatíveis, ao invés de adotar um termo tão abrangente que se esvai em si. Além do que, considerações mais específicas tendem à levar ao entendimento de que parte de condutas que aparentem ser distintas apenas por ocorrerem no meio virtual, ou no dito "ciberespaço", na realidade já tem respaldo na legislação em vigor.

Ainda assim, entende-se que a necessidade, bem como os procedimentos para se requerer a coleta, guarda, armazenamento e acesso a dados para fins de investigações que permitam comprovar a autoria e materialidade de delitos é um ponto comum quando se trata deste conceito amplo que se tem delineado para os chamados crimes cibernéticos. Contudo, a facilidade tecnológica de se recuperarem esses registros, bem como a fragilidade que o vazamento ou uso abusivo de dados pessoais pode representar para a manutenção das liberdades individuais, faz com que qualquer discussão sobre condutas criminosas utilizando-se das TICS, necessariamente, deva ser equilibradas com os princípios da presunção de inocência, da privacidade, da proteção de dados pessoais, do sigilo das comunicações, da liberdade de expressão e da diversidade . Seria contraditório à sua atividade fim que o Estado se valesse da violação sistemática e em massa de direitos individuais de milhões de inocentes, ou seja, cometesse graves violações de direitos, para combater crimes. Da mesma forma que seria incoerente combater ou banir o uso de determinadas tecnologias, inclusive úteis para a promoçao de direitos, devido ao mau uso das mesmas por poucos individuos voltados para atividades criminosas.

Os conceitos destacados nos itens a seguir visam esclarecer alguns conceitos legais e que dizem respeito ao entendimento de como funcionam as tecnologias para possibilitar esclarecimento suficiente para que se alcance esse balanço.

CAPÍTULO 4

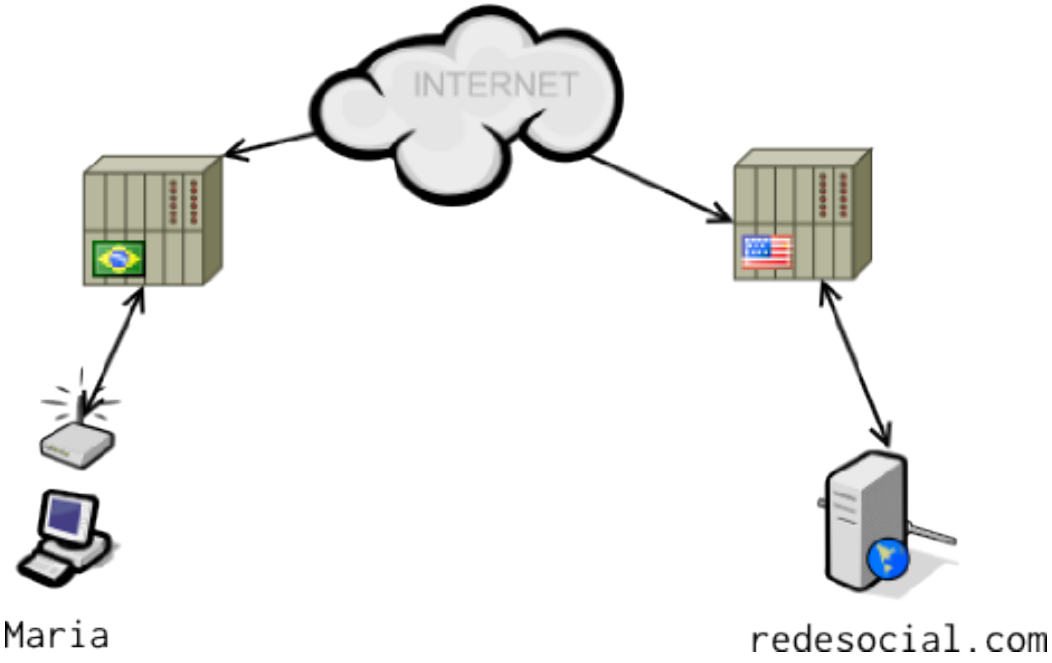
Marco Civil da Internet

O Marco Civil da Internet, Lei nº 12.965/2014, apresenta alguns conceitos e princípios específicos para a disciplina legal dos direitos e deveres nos usos da Internet no Brasil que não podem ser desconsiderados quando se trata de coibir crimes cibernéticos.

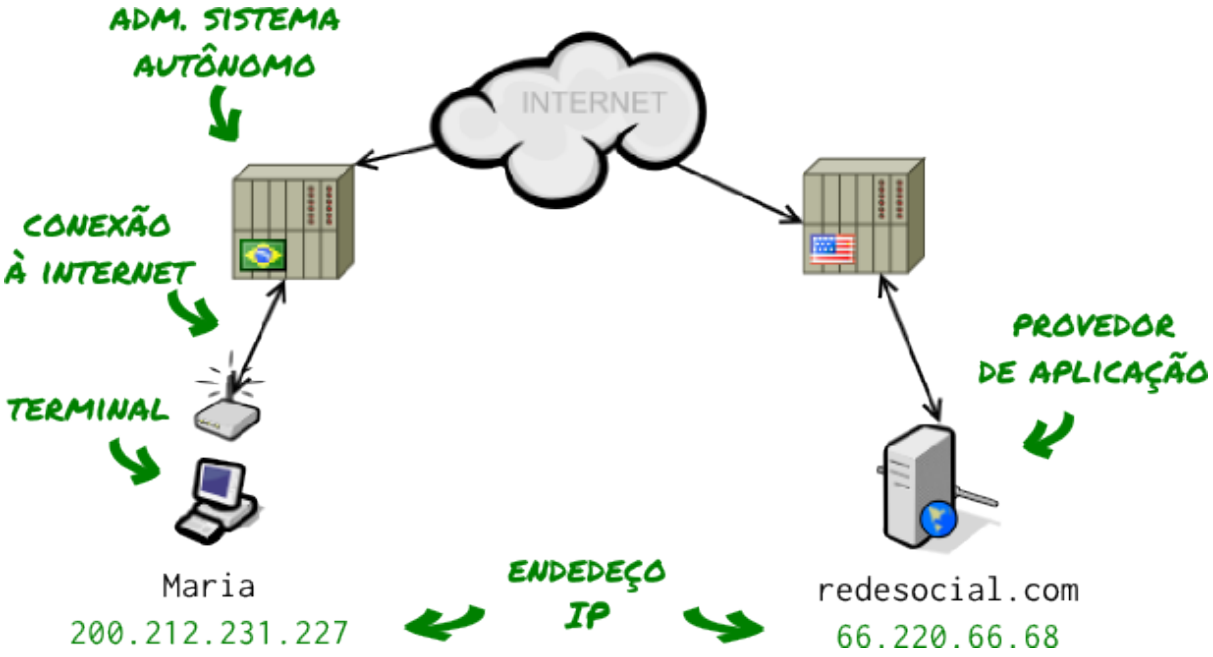
Destacamos abaixo alguns conceitos estabelecidos no Marco Civil, bem como sua aplicação na prática para melhor entendimento de como se dá o fluxo das comunicação na Internet. O Marco Civil, assim dispõe:

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

Para ilustrar, imagine um cenário em que Maria acessa, através da Internet, uma rede social hipotética `redesocial.com`, cujo servidor está nos EUA:



Aqui, destacamos os elementos de acordo com a terminologia do Marco Civil:



Para além da sessão de definições, a privacidade também aparece como princípio e direito fundamental no Marco Civil, entre seus dispositivos o texto estabelece:

- A "proteção à privacidade" e "a proteção de dados pessoais" aparecem listadas como princípios.
- A "inviolabilidade da intimidade e da vida privada", bem como a "inviolabilidade e sigilo, salvo por ordem judicial, do fluxo das comunicações e das comunicações armazenadas", aparecem como direitos assegurados.

- O texto estabelece o direito dos usuários ter “informações claras nos contratos de prestação de serviços, com detalhamento sobre as práticas de proteção aos registros armazenados”, bem como sobre “coleta, uso, armazenamento e tratamento de dados pessoais”. E ressalta ainda que “dados pessoais apenas poderão ser utilizados para finalidades que a) justifiquem a coleta; b) não sejam vedadas pela legislação e c) estejam especificadas nos contratos ou termos de uso.”
- Também são estabelecidos como direitos o “não fornecimento a terceiros de dados pessoais, salvo mediante consentimento livre, expresso e informado”. E o direito à, mediante requerimento, “exclusão definitiva dos dados pessoais que tivermos fornecido a determinada aplicação de internet, ressalvadas as hipóteses de guarda obrigatória”. Trata-se, portanto, de uma previsão genérica, do direito ao esquecimento, referente apenas aos dados que o usuário cede ao provedor de aplicação (não se trata de dados publicados por terceiros) e aplicável apenas no término da relação entre as partes.
- Por fim, o artigo 8 reconhece que a “garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet” e, como tal, declara que serão nulas as cláusulas contratuais que impliquem na “ofensa à inviolabilidade e ao sigilo das comunicações ou que não ofereçam o foro brasileiro como opção para solução de controvérsias. *[ANTIVIG-MCI-2-2014]* (Página 114)

Ou seja, a parte geral do Marco Civil, onde se estabelecem princípios, direitos e deveres dos usuários (Capítulos I e II), já traz referências importante ao direito à privacidade que devem ser levadas em conta como principios norteadores para qualquer atividades de combate a delitos que ocorram no meio virtual.

Mais detalhes sobre como implementar a proteção da privacidade, tendo em vista dados cadastrais, registros de conexão e de aplicações, estão previstos no capítulo III do Marco, que trata da provisao desses dois serviços. Numa mudança de última hora, o texto aprovado passou a determinar a retenção de ampos os tipos de registros, mas estabeleceu a necessidade de ordem judicial para acessar esses dados como salvaguarda.

4.1 Regulamentação do Marco Civil da Internet

O Marco Civil da Internet ainda não foi regulamentado; o decreto presidencial que definirá os detalhes sobre neutralidade de rede, guarda de registros de aplicação e o sistema de fiscalização para tornar efetivas as proteções da lei passou por consulta pública, encerrada no dia 1º de março.

Os principais pontos de discussão na consulta pública dizem respeito justamente à regulamentação da proteção da privacidade na guarda de registros de conexão e aplicações e estão compilados nessa visualização de dados feita no âmbito do projeto Oficina Antivigilância:

Um grupo de entidades da sociedade civil se reuniu para elencar entre si pontos comuns do decreto que devem necessariamente ser alvo de mudança ou de elaboração mais cuidadosa na versão final do texto. A carta circulou, foi endossada por mais grupos e apresentada como contribuição conjunta à consulta.

O texto da nota pública está disponível aqui (com ilustrações da Oficina Antivigilância): Regulamentação do Marco Civil: entenda e ajude a divulgar nossas contribuições.

Trilha 1: Home | Trilha 2: Marco Civil | Trilha 3: Dados Pessoais

PRIVACIDADE EM **CONSULTA**

PONTOS-CHAVE DO
MARCO CIVIL DA INTERNET

A partir de 2 dos 4 eixos da consulta pública do Marco Civil (Guarda de Registros e Privacidade), o *projeto Antivigilância* organizou as pautas em discussão por temas que dizem respeito à privacidade.

Clique nos círculos e visualize na tabela abaixo os debates existentes na plataforma sobre o tema selecionado

Guarda de Registros Privacidade na Rede

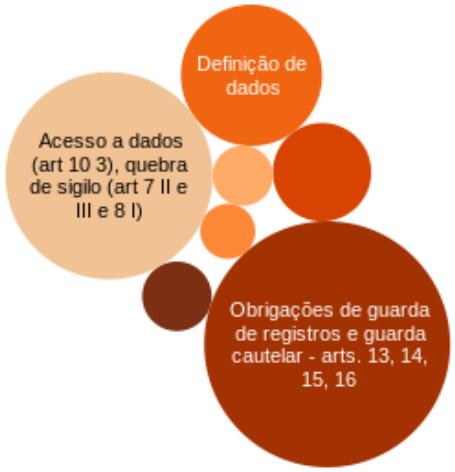


Fig. 4.1: Ilustração do ponto “Incongruências da Anatel fiscalizando aspectos da guarda de dados” da nota pública da sociedade civil

CAPÍTULO 5

Retenção de Registros de Conexão e Aplicações

5.1 Marco Civil da Internet

Retenção de dados segundo o **Marco Civil da Internet**
(Lei nº 12.965, de 23 abril de 2014)

	Provedor de conexão	Provedor comercial de aplicações	Provedor não comercial de aplicações
Tipo de dados a serem retidos	Registros de conexão à Internet	Registros de acesso a aplicações	
Obrigatoriedade de retenção dos dados	Obrigatório		Mediante requisição sem ordem judicial
Período de retenção dos dados	1 ano	6 meses	
Aumento do período de retenção	Mediante requisição sem ordem judicial		
Acesso aos dados retidos	Mediante ordem judicial		

Fonte: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm

Fig. 5.1: Tabela feita pelo Coletivo Saravá <https://www.sarava.org>

5.2 Violação de direitos?

Muito se negociou durante os vários anos de debate do Marco Civil da Internet sobre necessidade e prazos para a guarda de registros de conexão e de aplicações de internet até se chegar à situação do quadro acima. A obrigação de guarda registros de aplicação não saiu do texto produzido através das consultas públicas; ela foi introduzida quando o projeto de lei já estava no Congresso, tramitando em regime de urgência, em razão das revelações sobre práticas de vigilância em massa por parte do governo americano e aliados sobre as comunicações de autoridades e cidadãos no Brasil e no mundo.

Assim, a obrigação de guardar registros de aplicação foi introduzida nas últimas fases do debate e foi bastante criticada, tanto por representantes da sociedade civil por enfraquecer a proteção à privacidade dos usuários, como pelo setor privado, por gerar custos e responsabilidades adicionais relacionados ao armazenamento e a segurança de tal guarda.

Críticas que se apoiaram também no fato de que, em momento semelhante, mas sentido contrário, a Diretiva 24EC/2006 da União Européia, denominada de Diretiva de Retenção de Dados, foi julgada inconstitucional pela Corte Europeia em abril de 2014 *[ANTIVIG-24EC-2014]* (Página 115).

A análise "Marco Civil da Internet: seis meses depois, em que pé que estamos?" também retrata a polêmica da inclusão do artigo de retenção de dados:

> [...] Regimes de manutenção coletiva de dados, sem a necessidade de suspeita de ato malicioso, correompem as pré-condições a uma sociedade aberta e democrática, por enfraquecerem a confiança depositada pelos indivíduos na privacidade de suas comunicações e por criarem um risco permanente de perda e violação de dados. *[ARTIGO19-MCI-2015]* (Página 108)

PL215/2015, que encontra-se tramitando Câmara dos Deputados, se propõe a fazer justamente isso.

O fato é que, a cada dia, nossos computadores, celulares e uma gama de outros dispositivos coletam e processam mais e mais dados pessoais sensíveis – aqueles que revelam a "origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, bem como dados genéticos", como define o Anteprojeto de Proteção de Dados Pessoais do Ministério da Justiça.

Tais dispositivos também estão cada vez mais interconectados através de serviços como e-mail, redes sociais, aplicativos de mensagens e computação em nuvem, por onde todos estes dados (fotos, mensagens, documentos, geolocalização, buscas, e até passos dados durante o dia) são transmitidos e encaminhados para seus destinatários. Neste cenário, a retenção de dados se torna cada vez mais custosa.

Para definir o direito à privacidade neste novo contexto, o Conselho de Direitos Humanos das Nações Unidas publicou o relatório "The Right to Privacy in the Digital Age" ("privacidade na era digital"). Nele, é afirmado que a retenção de dados interfere na privacidade até mesmo quando os dados nunca são usados – no caso, se referindo aos programas de vigilância em massa da agência de segurança nacional dos EUA, a NSA (tradução e grifo nosso):

> Segue disso que qualquer captura de dados de comunicação é potencialmente uma interferência na privacidade e, além disso, que a coleta e retenção de dados de comunicações significa uma interferência com a privacidade quer ou não estes dados sejam posteriormente consultados ou usados. Mesmo a mera possibilidade das informações de comunicação serem capturadas cria uma interferência com a privacidade, com um efeito desencorajador (chilling effect) em direitos, incluindo aqueles à liberdade de expressão e associação. A própria existência de um programa de vigilância em massa então cria uma interferência com a privacidade. *[UN-PRIVACY-2014]* (Página 112)

O professor e pesquisador Daniel J. Solove, "um dos maiores especialistas em leis de privacidade" segundo o fórum de experts em TI SafeGov, descreve como o chilling effect causa danos à liberdade de expressão e de associação e à democracia (tradução nossa):

> Até a vigilância de atividades legais pode inibir as pessoas de engajarem-se nelas. O valor da proteção contra chilling effects não é medido simplesmente focando nos indivíduos em particular que foram impedidos de exercitar seus direitos. Os chilling effects causam danos à sociedade porque, entre outras coisas, reduzem a variedade de pontos de vista expressados e o grau de liberdade de se engajar em atividades políticas. *[SOLOVE-PRIVACY-2008]* (Página 114)

Mas a falta de sincronia com a tendência européia, internacionalmente conhecida com mais protetiva do exercício do direito à privacidade, bem como esse chilling effect na liberdade de expressão não são os únicos elementos de crítica. Abaixo destacamos alguns outros aspectos e soluções possíveis a serem consideradas também no mandato da CPI Ciber:

5.3 Custos

Reter dados em todos os provedores de conexão e aplicação comerciais também cria muitos custos novos: sistemas de armazenamento e backup, funcionários(as) para manter os sistemas e atender às demandas judiciais, e a segurança física e digital dos registros, que carregam em si grande valor comercial e muitas vezes poder político ou econômico.

Estes custos, além de prejudicarem o mercado como um todo, afetam especialmente as pequenas empresas e as *startups*, que devem arcar com as despesas de uma infraestrutura de armazenamento antes mesmo de terem um mercado consolidado.

Para armazenar uma quantidade cada vez maior de dados (e *backups* deles), os provedores precisam arcar com os custos de operação e manutenção de *datacenters*. Após o governo australiano passar uma lei de retenção de dados que obriga os provedores a armazenar os metadados de clientes por no mínimo 2 anos, os custos estimados pela indústria para a adaptação do setor de telecomunicações se encontram entre 300 e 700 milhões de dólares australianos *[KNOTT-WROE-2015]* (Página 111). Este cálculo é feito em cima de 12,5 milhões de assinaturas de Internet na Austrália; de acordo com pesquisa do NIC.br e Cetic.br, em 2014 haviam mais de 32 milhões de domicílios com acesso à Internet no Brasil *[TICDOMICILIOS-2015]* (Página 115).

5.4 Vazamentos

Mesmo seguindo padrões e boas práticas de segurança, nenhum sistema é completamente seguro e o risco de invasões e vazamentos é sempre presente.

O vazamento de dados através de invasões, erros técnicos, corrupção de funcionários e outros fatores têm atingido até mesmo em gigantes do setor – como Sony, Target, Adobe, Ebay,

Vodafone, SnapChat, Twitter, Facebook, Steam, Blizzard e dezenas de outras presentes numa compilação de grandes vazamentos de bancos de dados dos últimos anos.

A natureza da segurança digital faz com que vulnerabilidades novas para plataformas antes consideradas seguras surjam o tempo inteiro; com trabalho especializado, custos de serviços e equipamento,e uma série de práticas e rotinas de segurança, é possível proteger um sistema da maior parte das ameaças; mesmo o trabalho dedicado de uma equipe, no entanto, pode ser contornado por um adversário com determinação e recursos suficientes.

Se o problema é alarmante até mesmo para organizações estabelecidas e cautelosas, é mais ainda para provedores em todo o país e no exterior que têm, em média, muito menos recursos e incentivos para proteger seus sistemas. Obrigar a guarda de registros aumenta o grau e o alcance dos danos que vazamentos podem causar aos provedores e seus clientes.

Também devem ser contabilizados nos custos da retenção de dados aqueles associados aos vazamentos, como os gastos jurídicos de retratação, o esforço e a inconveniência para um indivíduo de ter seus dados expostos (frequentemente com danos econômicos e morais, e por vezes até psicológicos ou fatais) e do impacto social da insegurança geral das interações *online*.

5.5 Metadados

Os metadados também são protegidos pelo sigilo das comunicações, por serem tão sensíveis quanto o conteúdo, e por vezes mais fáceis de serem usados para revelar informações e padrões de comportamento de indivíduos e organizações.

O termo *metadado*, "dado sobre outros dados", significa tudo que é trafegado pela rede ou armazenado em disco que não seja o *conteúdo* em si de uma mensagem ou arquivo (como o corpo de um e-mail ou os *pixels* de uma imagem), e sim informações de roteamento, categorização ou descrição.

No nível da rede TCP/IP, os roteadores que compõe a Internet precisam saber de onde vem e para onde vai um determinado pacote para poder encaminhá-lo de forma correta. Os endereços IP de origem e destino são então os *metadados* dos pacotes.

Já no nível de serviços, tomando o e-mail como exemplo, os endereços de origem e destino de uma mensagem (como `fulana@camara.gov.br` e `beltrano@exemplo.adv.br`), a data e hora de envio e o assunto ("Preciso de ajuda"), são alguns de seus *metadados*.

A carta Princípios Internacionais sobre a Aplicação Dos Direitos Humanos na Vigilância Das Comunicações, o "resultado de uma consulta global com grupos da sociedade civil, da indústria e especialistas internacionais em questões jurídicas, políticas e tecnológicas relacionadas à Vigilância das Comunicações", explica o poder dos metadados:

> Os metadados de comunicações podem criar um perfil de vida do indivíduo, incluindo questões médicas, pontos de vista políticos e religiosos, associações, interações e interesses, revelando tantos detalhes quanto — ou ainda mais — do que seria perceptível a partir do conteúdo das comunicações. Apesar do vasto potencial de intromissão na vida do indivíduo e do efeito desencorajador ("*chilling effect*") sobre a associação política e de outra natureza, as leis, regulamentos, atividades, poderes ou autoridades frequentemente atribuem aos metadados de comunicações um nível de proteção menor e não impõem restrições suficientes a como eles podem ser usados posteriormente pelos Estados. *[13-PRINCIPIOS]* (Página 113)

Dennys Antonialli, diretor executivo do InternetLab, exemplificou muito bem tal poder em audiência pública dessa CPI ao mostrar a "rede social" que é possível extrair através somente dos endereços de origem e destino e da data/hora de seus e-mails através da ferramenta Immersion, desenvolvida no Massachusets Technology Institute (MIT):

A Corte Interamericana de Direitos Humanos (CIDH) explicitou, no caso *Escher e outros vs. Brasil* que os metadados também são abarcados na proteção à privacidade:

> [O direito à privacidade] aplica-se às conversas telefônicas independentemente do conteúdo destas, inclusive, pode compreender tanto as operações técnicas dirigidas a registrar esse conteúdo, mediante sua gravação e escuta, como qualquer outro

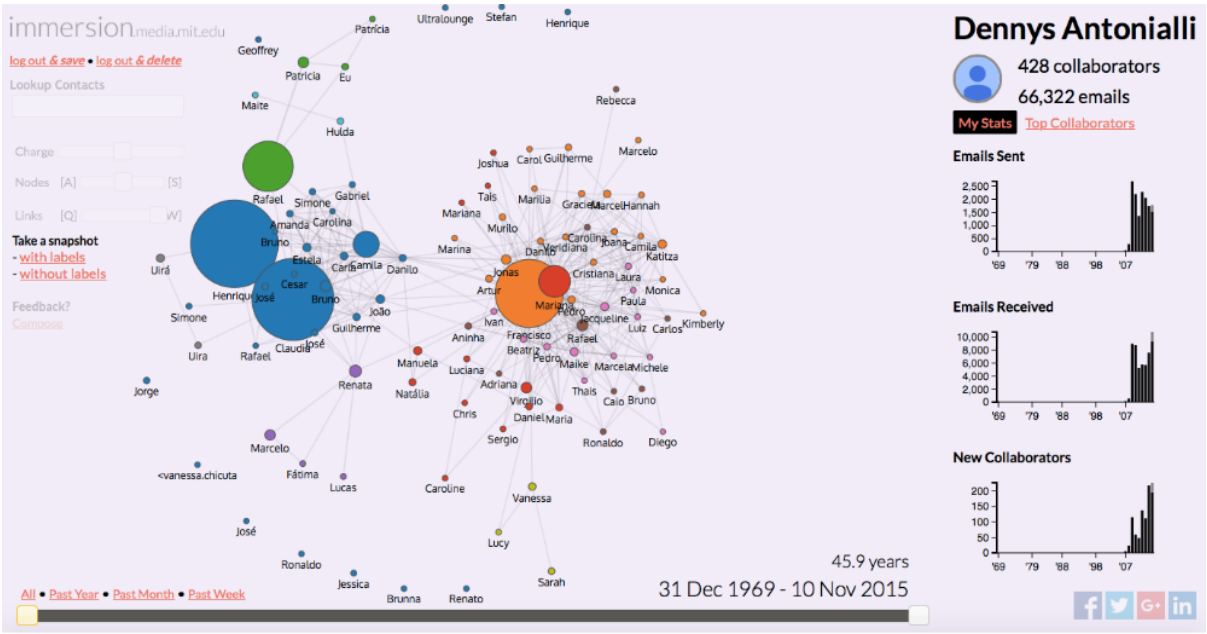


Fig. 5.2: Rede de contatos de Dennys. Cada cor representa um círculo social diferente (por exemplo, "família" e "colegas de trabalho"); o tamanho do círculo é a quantidade de mensagens trocadas e as ligações entre os círculos são feitas quando as pessoas estão em cópia numa mesma mensagem.

> elemento do processo comunicativo, como, por exemplo, o destino das chamadas que saem ou a origem daquelas que ingressam; a identidade dos interlocutores; a frequência, hora e duração das chamadas; ou aspectos que podem ser constatados sem necessidade de registrar o conteúdo da chamada através da gravação das conversas. Finalmente, a proteção à vida privada se concretiza com o direito a que sujeitos distintos dos interlocutores não conheçam ilicitamente o conteúdo das conversas telefônicas ou de outros aspectos, como os já elencados, próprios do processo de comunicação *[CIDH-2009]* (Página 110)

5.6 Retenção mínima

A melhor medida de segurança contra o vazamento de dados é não guardá-los. Uma política de retenção mínima de dados, onde os sistemas são desenhados para coletar o mínimo de informações necessárias para seu objetivo, fortalece a privacidade, a liberdade de expressão e a segurança de toda a sociedade ao remover pontos de acúmulo de dados, que por seu valor econômico e político são visados por criminosos, espiões e agências de inteligência de diversos países.

Para maior proteção de direitos fundamentais como a privacidade e a liberdade de expressão, e também para maior segurança dos usuários contra vazamentos de dados, a política de reter o mínimo de dados para o funcionamento do serviço é ideal. Como explicou Claudia Melo para o Technology Radar, um estudo da empresa de software ThoughtWorks:

> Diversos setores do mercado brasileiro vêm considerando Big Data uma das apostas para alavancar o negócio e melhorar o relacionamento com os clientes. Se por um lado a tecnologia permite que todos os seus dados, interesses e interações sejam armazenados e analisados, por outro há sérios riscos relacionados à privacidade das pessoas", afirma Claudia Melo, Diretora de Tecnologia da ThoughtWorks Brasil. "Nós defendemos que as empresas devem armazenar somente o mínimo necessário de informações de seus clientes, uma política que alemães denominam de *datensparsamkeit*, afirma Martin Fowler, cientista chefe da ThoughtWorks. *[THOUGHTWORKS-2014]* (Página 115)

O conceito alemão de **datensparsamkeit** está em sintonia com o que Cristiana Gonzalez, pesquisadora do Instituto de Defesa do Consumidor, manifestou em audiência pública dessa CPI: "Sistemas deveriam ser desenhados para terem o mínimo de vigilância necessário e coletar o mínimo de informação necessária para determinado objetivo".

CAPÍTULO 6

Criptografia

A criptografia é uma técnica matemática que permite, entre outras coisas, garantir a confidencialidade, a autenticidade e a integridade de mensagens e documentos.

Criptografia é o estudo das técnicas de se **comunicar de forma segura** quando se tem **alguém escutando o canal de comunicação**. Historicamente, várias formas rudimentares de substituição de letras foram usadas para transmitir segredos entre impérios. Hoje em dia, qualquer técnica de criptografia relevante é feita através de manipulações matemáticas, derivados da teoria dos números, que transformam um bloco de informação contendo uma mensagem, imagem, documento, etc, em um bloco de tamanho semelhante mas completamente ininteligível.

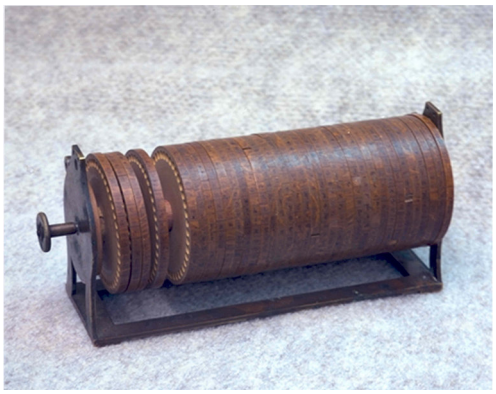


Fig. 6.1: Um cilindro de Jefferson (ou cilindro cifrante), um dispositivo "composto por 26 discos de madeira que giram livremente ao redor de um eixo central de metal", inventado por Thomas Jefferson (que seria presidente dos EUA) em 1795. *[VICKY-JEFFERSON-2007]* (Página 116)

O que **impede a pessoa adversária** (nome técnico dado a quem tenta quebrar a mensagem) **de ler a mensagem** não é o algoritmo de criptografia em si, isto é, às instruções de como embaralhar a mensagem. Em vez de proteger o método de embaralhamento, quem deseja sigilo para sua mensagem precisa manter somente um pequeno, mas importante ingrediente do processo em segredo: a **chave de criptografia** (no caso do cilindro de Jefferson, a chave é a ordem das letras nos discos).

A isto se dá o nome de criptografia simétrica, pois que os dois lados da conversa possam trocar mensagens de forma segura, têm que combinar a chave de antemão – pois de nada adianta compartilhar esse segredo num canal que se assume estar grampeado.

Com o advento da criptografia de chave pública, isso tornou-se desnecessário; os pesquisadores Whitfield Diffie e Martin Hellman criaram um sistema onde um **par de chaves** é gerado para cada lado da conversa; uma delas (a chave "pública") serve para "lacrar" a mensagem; a outra (a chave "secreta" ou "privada") serve para "abrir" tais mensagens. Dessa maneira, duas pessoas podem **compartilhar suas chaves públicas por um canal inseguro** sem que se possa usá-las para descriptografar as mensagens que passam em seguida.

Fig. 6.2: Como funciona a criptografia de chave pública. Imagem da Free Software Foundation *[FSF-Jpp-GNUPG-2014]* (Página 110)

6.1 Ubíqua e vital

Algoritmos de criptografia são blocos de construção essenciais para a segurança de nossas operações cotidianas na Internet, da infraestrutura de energia e das comunicações do governo, das transações bancárias e de mecanismos críticos do setor financeiro, e de muitas outras atividades importantes da sociedade.

Quando se usa qualquer serviço moderno de comunicação pela Internet, como Whatsapp e Gmail, ou sistemas de online banking, a criptografia está presente. Além de prover o sigilo de

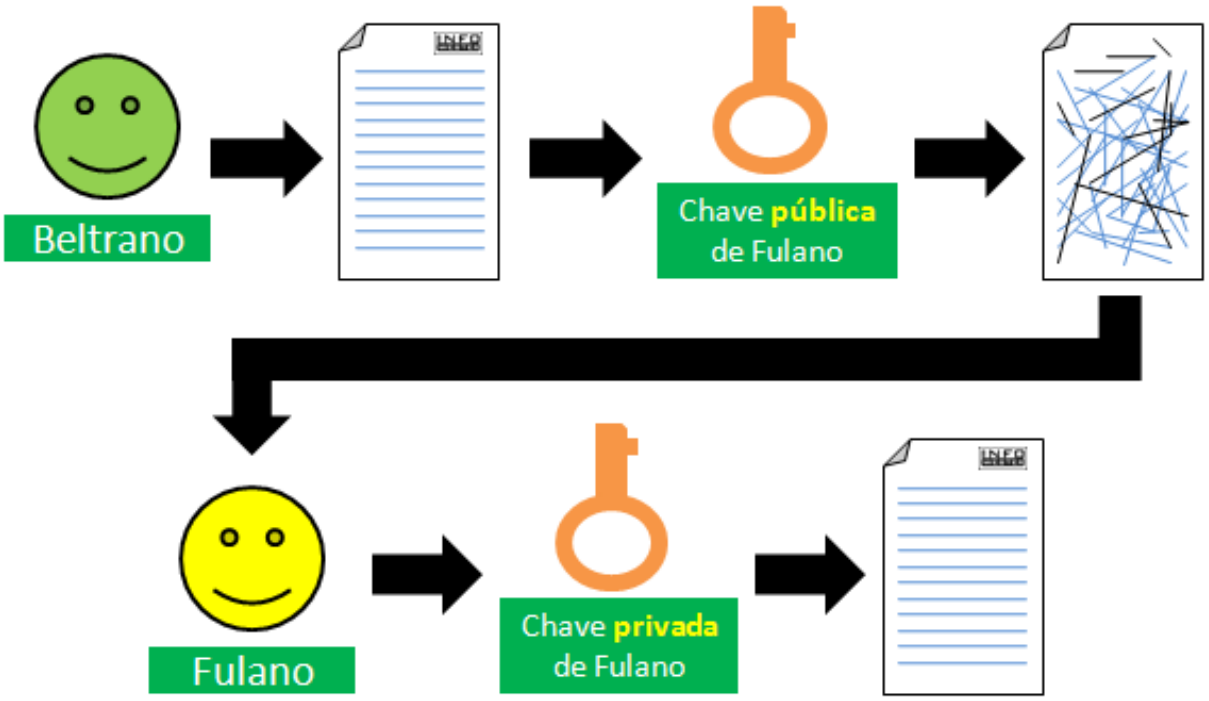


Fig. 6.3: Como funciona a criptografia de chave pública. Imagem do InfoWester *[INFOWESTER-2009]* (Página 108)

mensagens, a mesma técnica matemática pode ser usada também para autenticação: uma pessoa ou organização pode assinar uma mensagem digitalmente usando sua chave secreta, e quem quer que possua sua chave pública (que pode estar publicada no *site* da pessoa/organização) será capaz de confirmar que ela veio de fato de quem diz ter vindo. Aplicativos que usam criptografia fim-a-fim / ponta-a-ponta (como o Whatsapp, o Signal, o PGP e o GnuPG) criam essas chaves no próprio aparelho das pessoas que querem se comunicar. O servidor, então, passa a não ter acesso ao conteúdo das mensagens, embora ainda tenha a alguns metadados (como o dia e hora da mensagem, remetente e destinatário).

Veja também:

Retenção de Registros de Conexão e Aplicações > Metadados (Página 21)

A técnica conhecida como *forward secrecy* (numa tradução livre, "sigilo daqui para frente"), que vem sendo também implementada nos softwares de criptografia mais modernos, consiste em criar diversas chaves, uma por mensagem, apagando-as logo em seguida dos aparelhos. A chave secreta que fica armazenada no dispositivo serve somente para os primeiros passos da conexão até se estabelecer a primeira chave efêmera a ser usada na conversa. Dessa maneira, mesmo o acesso à chave permanente não permite decifrar o conteúdo que passa pelo servidor, e quebrar a conversa passa a envolver quebrar dezenas ou centenas de chaves em vez de uma só.

É importante lembrar que a criptografia de chave pública e a técnica de *forward secrecy*, embora impeçam que as mensagens retidas sejam acessíveis em uma futura investigação policial, aumentam consideravelmente não só a **privacidade** dos(as) usuários(as) finais frente à **indústria da coleta de dados e da publicidade** e ao tratar de **assuntos sensíveis**, como também a **segurança frente a fraudes** cometidas por *crackers*, o **vazamento das informações** do servidor decorrentes de uma invasão, erro técnico ou **má fé**, e à **sistemas de monitoramento e**

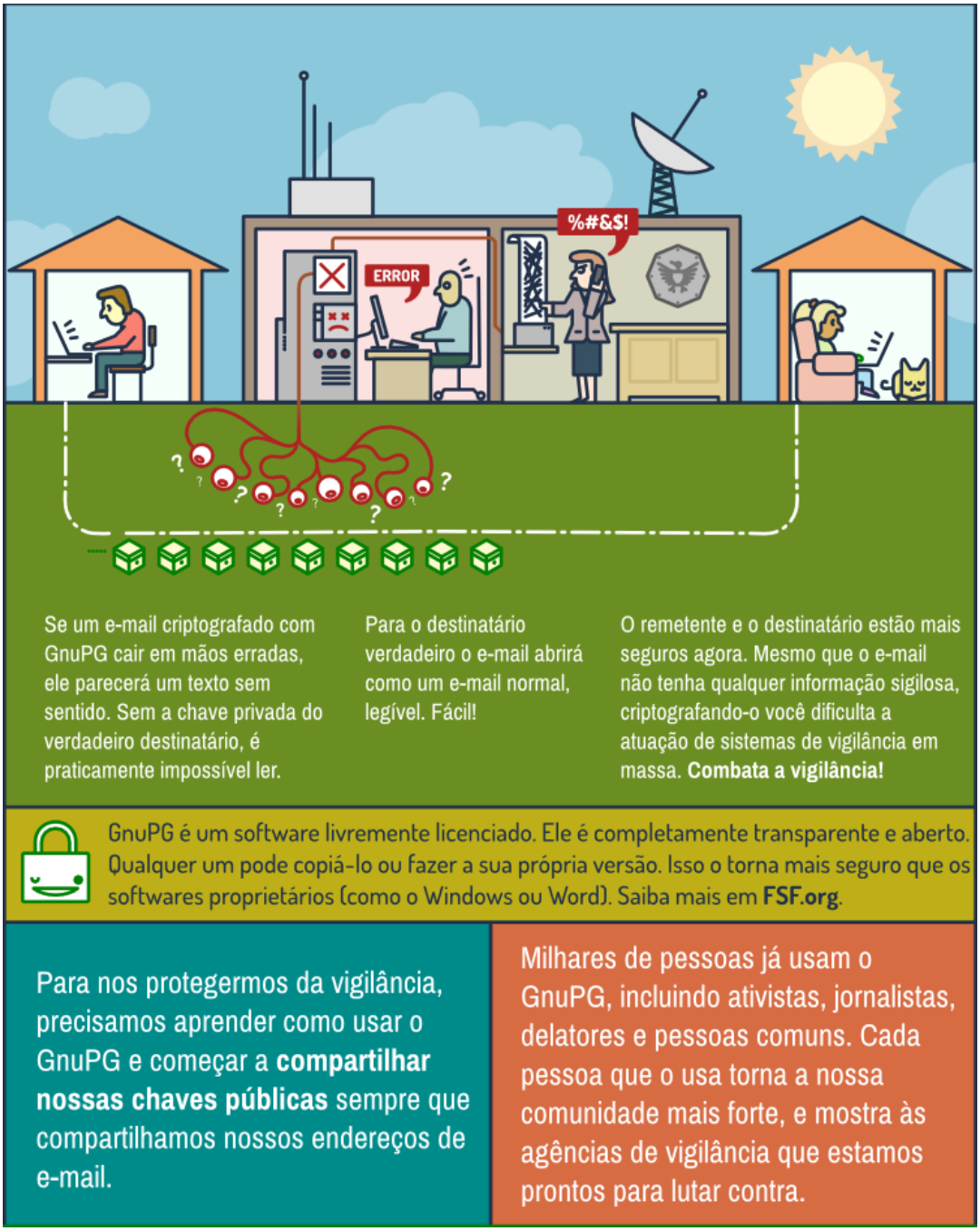


Fig. 6.4: Como a criptografia de chave pública protege nossas comunicações e ações rotineiras na Internet de criminosos e agências de inteligência – no caso, com o software livre GnuPG. Imagem da Free Software Foundation *[FSF-Jpp-GNUPG-2014]* (Página 110)

vigilância estrangeiros como os mantidos pela Agência de Segurança Nacional dos EUA e amplamente expostos na mídia após denúncias de Edward Snowden.

Veja também:

Retenção de Registros de Conexão e Aplicações > Vazamentos (Página 20)

6.2 Sem porta dos fundos

Se bem implementada, a criptografia impede que qualquer pessoa de fora da converesa acesse o conteúdo das mensagens – até mesmo órgãos de investigação policiais ou judiciários. Alguns destes órgãos não concordam com esta possibilidade e exigem acesso especial para autoridades ou algum tipo de "chave dourada" que possa quebrar a criptografia em uma emergência.

Há duas possibilidades técnicas para fazer isto funcionar: um "backdoor" na criptografia ou um mecanismo de "key escrow", onde todas as mensagens criptografadas devem ser legíveis pela "chave da polícia". Se referindo a ambos os mecanismos, o Relator Especial das Nações Unidas para a Liberdade de Expressão disse em 2015 que "os Estados devem evitar todas as medidas que enfraqueçam a segurança da qual os indivíduos desfrutam online".

O uso da criptografia caminha de mãos dadas com as recomendações do Relator Especial das Nações Unidas para a Liberdade de Expressão, David Kaye: "**os Estados devem evitar todas as medidas que enfraqueçam a segurança da qual os indivíduos desfrutam online**, como *backdoors*, padrões mais fracos de criptografia e *key escrows*" *[KAYE-2015]* (Página 111).

Backdoors, traduzido ao pé da letra como "porta dos fundos", são trechos escondidos de um programa que permitem que quem o desenvolveu ganhe acesso ao computador que o executa ou possa quebrar a sua criptografia.

Já **key escrows** são mecanismos onde a justiça ou outro poder investigativo também possui acesso a chaves que possam abrir as mensagens. À primeira vista, essa é uma maneira simples de resolver a questão, mas os desdobramentos técnicos de como colocar isso em prática de forma a não permitir que tais mecanismos sejam burlados quanto evitar abuso por parte das autoridades de investigação trazem problemas que podem ser ainda maiores do que a impossibilidade de fazer grampos.

6.3 Chaves debaixo do carpete

Um extenso estudo sobre backdoors e key escrows feito por especialistas em computação e criptografia conclui que "tal acesso abriria portas pelas quais criminosos e nações mal intencionadas poderiam atacar os mesmos indíviduos que a polícia deseja defender".

Em julho de 2015, em uma resposta à demanda de representantes do FBI e da Casa Branca às empresas de tecnologia para que inventassem uma maneira de que a criptografia de seus aplicativos e dispositivos pudesse ser aberta com uma "chave dourada", disponível sob ordem judicial

(semelhante ao desentendimento entre o Whatsapp e os(as) juízes brasileiros(as) que demandaram dados de pessoas), um grupo de especialistas em ciência da computação e criptografia se reuniu para escrever "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications" (tradução livre: "Chaves Debaixo do Carpete: Exigindo a Insegurança ao Requerer Acesso do Governo a Todos os Dados e Comunicações"). Em suas 32 páginas, o estudo analisa várias formas propostas pelo governo estadunidense de tornar a criptografia quebrável por autoridades competentes, e a conclusão é clara (tradução e grifos nossa):

> Mesmo que cidadãos necessitem dos agentes da lei para se protegerem no mundo digital, todos os legisladores, empresas, pesquisadores, indivíduos e agentes têm a obrigação de trabalhar para tornar nossa infraestrutura global de informações mais segura, confiável e resiliente. A análise deste relatório das **demandas da polícia por acesso excepcional às comunicações e dados privados** mostra que **tal acesso abriria portas pelas quais criminosos e nações mal intencionadas poderiam atacar os mesmos indivíduos que a polícia deseja defender**. Os custos seriam substanciais, os danos à inovação seriam severos, e as consequências no desenvolvimento econômico seriam difíceis de prever.

6.4 Um exemplo vivo: Juniper e o backdoor do backdoor

Seis meses depois do estudo Keys Under Doormats, a gigante da tecnologia Juniper Networks anunciou que havia encontrado um backdoor em seu algoritmo de criptografia; o detalhe é que a falha, introduzida e explorada por criminosos até o momento desconhecidos, se aproveitava de OUTRA vulnerabilidade introduzida sorrateiramente pela NSA para que a agência pudesse vigiar o tráfego da rede quando necessário para seus objetivos.

A falha, presente no sistema ScreenOS usado em equipamentos de rede NetScreen®, permitia que alguém com acesso a uma determinada *chave secreta* poderia quebrar a criptografia da VPN, usada para acessar a Internet de forma segura em redes públicas ou hostis, e ter acesso às comunicações que passam pelo cabo ou pelas ondas de rádio.

Tal esquema foi possível se aproveitando do fato de que o ScreenOS *já utilizava* um algoritmo com *backdoor*, mas neste caso implantado pela NSA: o algoritmo conhecido como "Dual-EC", que segundo o pesquisador de segurança Adam Langley "foi um esforço da NSA para introduzir um gerador de números pseudo-aleatórios com um *backdoor* que, dado o conhecimento de uma chave secreta, permitia a um adversário observar a saída do gerador e prever seus resultados futuros". Como a imprevisibilidade, a entropia, é o principal ingrediente da criptografia, esta capacidade permite quebrar facilmente a proteção da VPN.

CAPÍTULO 7

Interceptação

7.1 Panorama Legal

No artigo "Interceptações e Privacidade: novas tecnologias e a Constituição", o ministro do STF Gilmar Ferreira Mendes e o juiz federal Jurandi Borges Pinheiro fazem "uma análise crítica da legislação brasileira sobre interceptações telefônicas e telemáticas [...] em face dos avanços tecnológicos que se multiplicam nessa área e da garantia constitucional do direito à privacidade". *[MENDES-PINHEIRO-2015]* (Página 111)

Os autores identificam três leis que regem a interceptação no Brasil: a Constituição de 1988, a Lei de Interceptações Telefônicas (LIT, nº 9.296/96) e o Marco Civil da Internet (lei nº 12.965/2014).

A análise "Vigilância das Comunicações pelo Estado Brasileiro" *[INTERNETLAB-2016]* (Página 108) vai além destas três e nos traz também a Lei Geral das Telecomunicações (LGT, nº 9.472/1997), que impede o acesso às comunicações e restringe o uso e a divulgação de (meta)dados de utilização do usuário pelas prestadoras de serviço de telecomunicação.

7.1.1 Constituição de 1988

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> [...]
>
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Fig. 7.1: Vigilância das Comunicações pelo Estado Brasileiro, relatório feito pelo centro de pesquisa InternetLab em parceria com a Electronic Frontier Foundation.

7.1.2 Lei de Interceptações Telefônicas

> Pela Lei 9.296/96, interceptações de comunicações telefônicas e de sistemas de informática e telemática podem ocorrer mediante ordem judicial, de ofício ou por requerimento de autoridade policial ou do Ministério Público, quando há indícios razoáveis de autoria ou participação em infração penal punida com pena de reclusão e indisponibilidade de outros meios de produção de prova (arts. 1o e 2o). *[INTERNETLAB-2016]* (Página 108)

7.1.3 Marco Civil da Internet

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;o
>
> 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;

[...]

Veja também:

Marco Civil da Internet (Página 13)

7.1.4 Lei Geral das Telecomunicações

Art. 3° O usuário de serviços de telecomunicações tem direito:

[...]

V - à inviolabilidade e ao segredo de sua comunicação, salvo nas hipóteses e condições constitucional e legalmente previstas;

[...]

IX - ao respeito de sua privacidade nos documentos de cobrança e na utilização de seus dados pessoais pela prestadora do serviço;

[...]

Art. 72. Apenas na execução de sua atividade, a prestadora poderá valer-se de informações relativas à utilização individual do serviço pelo usuário.

§ 1° A divulgação das informações individuais dependerá da anuência expressa e específica do usuário.

§ 2° A prestadora poderá divulgar a terceiros informações agregadas sobre o uso de seus serviços, desde que elas não permitam a identificação, direta ou indireta, do usuário, ou a violação de sua intimidade.

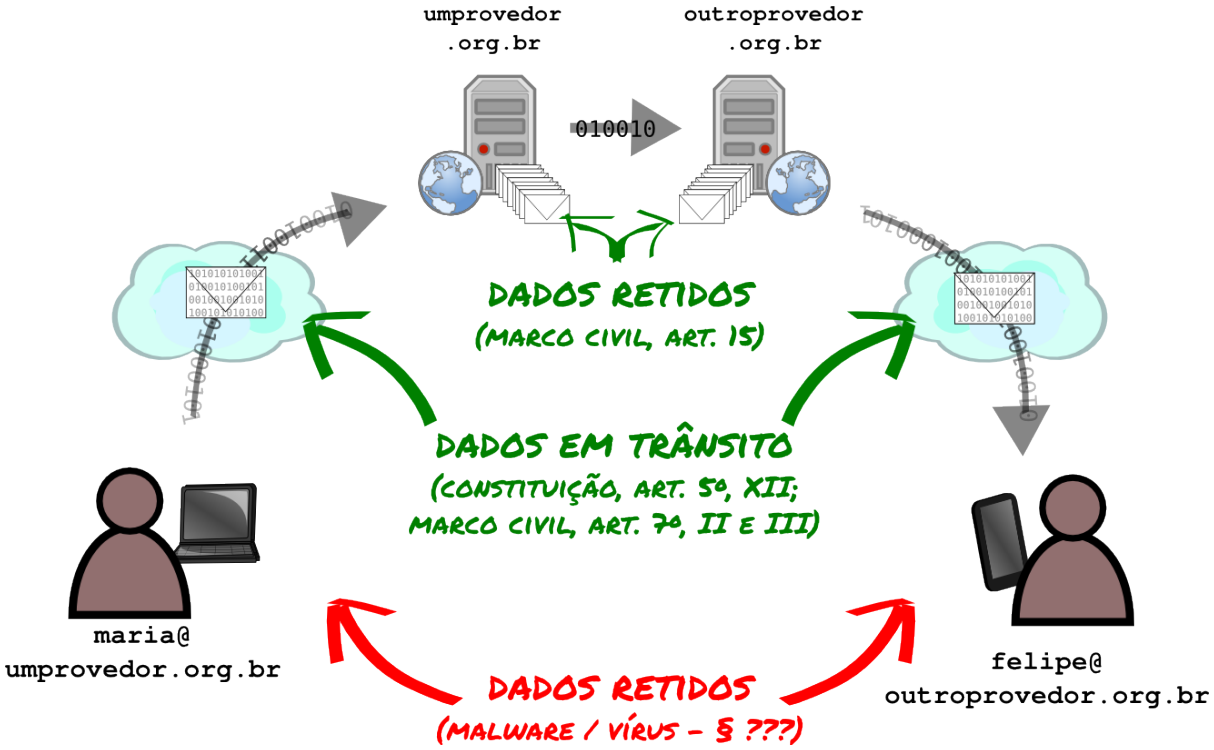
7.2 Comunicações em trânsito vs. comunicações armazenadas

O Supremo Tribunal federal, através do recurso extraordinário nº 418.416/SC, entendeu que "a proteção a que se refere o art. 5º, XII [da Constituição], é da 'comunicação de dados' e não dos dados em si considerados", ainda quando armazenados em computador *[MENDES-PINHEIRO-2015]* (Página 111). No entanto esta decisão, tomada em 2010, não levou em conta a já crescente e hoje exponencialmente maior prática de gerar e armazenar em bancos de dados "na nuvem" informações que se relacionam com nossa vida de múltiplas e reveladoras maneiras.

Efetivamente, a decisão separa as comunicações em categorias; podemos chamá-las de *comunicação em trânsito* (onde se dá a interceptação tradicional, onde se escuta o canal e grava o que trafega por ele) e *comunicação armazenada*, todas as mensagens e dados que permanecem nos servidores ou no computador dos(as) usuário(as).

Já o caso do acesso a computadores ou smartphones (onde ficam, por exemplo, registros de conversas passadas e históricos de navegação), não há legislação específica. O acesso legal se dá tradicionalmente através de operações de *busca e apreensão*, mas há uma tendência crescente

preocupante de uso de *malware*, ou *cavalos de tróia*, para infectar computadores e controlá-los remotamente.



O ministro do STF Gilmar Mendes e o juiz federal Jurandi Borges Pinheiro, em sua análise conjunta "Interceptações e Privacidade - Novas Tecnologias e a Constituição", vêem com preocupação o acesso aos dados (registros, documentos, mensagens, agendas, anotações...) de usuários armazenados em servidores *online*, por violar o que a Corte Constitucional alemã chamou de "direito à integridade de sistemas de tecnologia da informação" no caso conhecido como *Online-Durchsuchungen*: (grifos nossos):

> Especificamente em relação ao sigilo das comunicações, predominava no direito alemão, no mesmo sentido da jurisprudência do STF, há pouco examinada, o entendimento de que seu objeto é o conteúdo da comunicação no momento em que ela se realiza e não os dados armazenados após a sua transmissão. A razão de ser dessa distinção é que as informações armazenadas em qualquer dispositivo, após a sua transmissão, já não estariam mais expostas aos perigos que normalmente resultam da vulnerabilidade dos dados durante o processo de comunicação.
>
> No caso *Online-Durchsuchungen* , contudo, foi ressaltado que os **computadores estão presentes em todas as áreas de vida moderna** e são cada vez mais **essenciais ao desenvolvimento da personalidade**. Todavia, enquanto criam novas oportunidades, também colocam em **risco** os seus usuários. Dessa forma, **tendo em conta a possibilidade de busca e apreensão remota de dados já armazenados, sem a necessidade, portanto, da apreensão do computador, a proteção com base na distinção entre transmissão e armazenamento passou a se mostrar insuficiente**.
>
> Diante dessa nova realidade, adotou o Tribunal o conceito de *sistema de tecnologia da informação* como um sistema com capacidade de conter dados técnicos a

> um ponto que fosse possível ter conhecimento de uma substancial parcela da vida de um indivíduo e noção significativa de sua personalidade. Com base nesse conceito, assentou a Corte que a confidencialidade e **a integralidade dos sistemas de tecnologia da informação configuram direito fundamental comparável à inviolabilidade do domicílio**.
>
> [...]
>
> Ressaltou a Corte, todavia, que "busca *on-line*" de informações poderia, nesses casos, ser **justificada com a finalidade de prevenir práticas criminosas, mediante autorização judicial** e desde que observados os **requisitos constitucionais** de clareza e determinação jurídica.
>
> [...]
>
> Essa nova concepção do direito à privacidade, sem precedente no direito alemão, **serviu como forma de preencher uma lacuna até então existente e passou a ser um marco não apenas na Alemanha, mas em toda a Europa**. *[MENDES-PINHEIRO-2015]* (Página 111)

Embora o Marco Civil da Internet coloque limites – principalmente após ser regulamentado – no acesso aos registros de conexão e aplicação, os requisitos para acesso ainda não estão tão claros quanto necessários para um artifício tão intrusivo, e a possibilidade de acesso aos dados armazenados "na nuvem" (que não os registros) está em uma zona de insegurança jurídica, como apontam também Gilmar Mendes e Jurandi Borges Pinheiro (grifos nossos):

> [após citar e explicar os trechos do Marco Civil que tratam de guarda de registros:] O citado diploma legal assegura aos usuários da internet, expressamente, não apenas o sigilo do fluxo das comunicações, já objeto de regulamentação pela Lei n. 9.296/96, como também a inviolabilidade e o sigilo dos dados armazenados (art. 7º, II e III), os quais somente podem ser disponibilizados mediante ordem judicial (art. 10, § 2º).
>
> [...]
>
> Como se percebe, contamos, agora, com um conjunto de dispositivos legais que busca proteger, com razoável detalhamento, as operações de coleta e armazenamento de dados, os registros de conexão, bem como os conteúdos acessados, baixados ou transmitidos. Cabe destacar, como ponto positivo entre as medidas adotadas, a expressa exigência de autorização judicial para qualquer forma de acesso a esses dados, preservando-se, com isso, a privacidade do usuário.
>
> [...]
>
> Cabe ressalvar, contudo, a **insuficiente proteção da nova lei por não especificar os requisitos a serem observados na autorização judicial de acesso aos dados armazenados, que podem abranger, conforme há pouco se destacou, não apenas dados obtidos pela Internet, como, também, arquivos gerados e mantidos em pastas locais sem conexão com aplicativos on-line**. *[MENDES-PINHEIRO-2015]* (Página 111)

Seria interessante, então, ter como um dos encaminhamentos da CPI uma melhor regulamentação ou doutrina jurídica sobre a "interceptação" de comunicações e dados armazenados *online*,

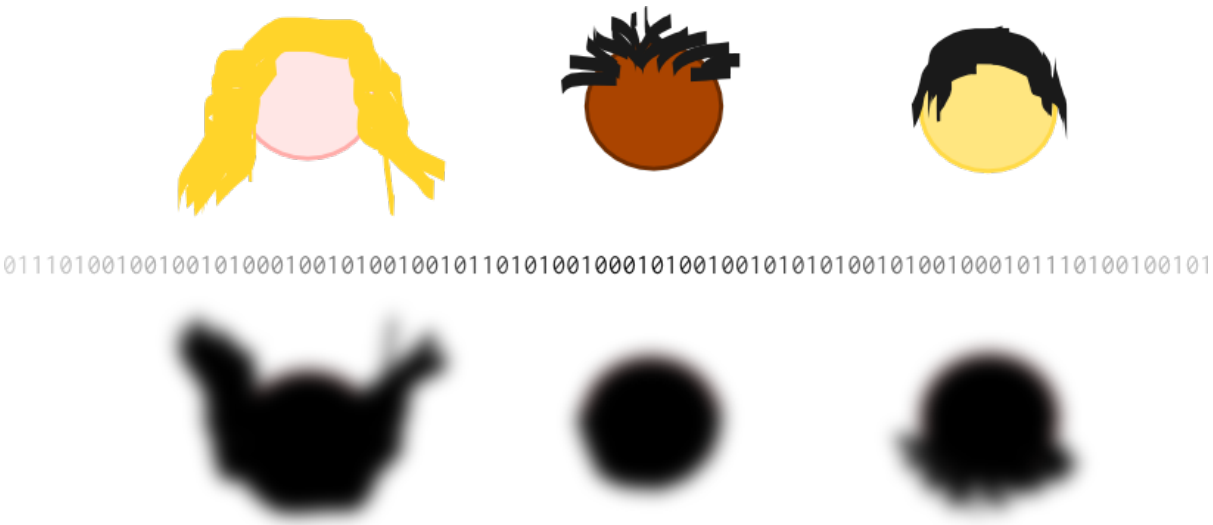
além dos registros de conexão e aplicação já tratados pelo Marco Civil da Internet, bem como um esclarecimento sobre os contextos ou as autoridades que podem requisitar acesso aos registros dos provedores de conexão e aplicação. O ideal é caminhar em direção a um direito semelhante ao de "integralidade dos sistemas de tecnologia da informação" da Alemanha.

Veja também:

- ***Retenção de Registros de Conexão e Aplicações*** **(Página 18)**
  - *Violação de direitos?* (Página 18)
  - *Metadados* (Página 21)
- ***Marco Civil da Internet*** **(Página 13)**
  - *Regulamentação do Marco Civil da Internet* (Página 15)

CAPÍTULO 8

Anonimato Online



8.1 Vedação constitucional

Liberdades de manifestação vs. acesso à informação

Diferentemente de outros países democráticos, a Constituição no Brasil proíbe expressamente o anonimato, mantendo previsão existente desde 1891. Entretanto, o texto de 1988 veda o anonimato exclusivamente no âmbito da manifestação do pensamento.

Portanto, **não há nenhuma proibição de que haja anonimato no acesso à informação, prática corrente não só na Internet, mas também na vida presencial**: ninguém precisa se identificar para ir o teatro ou ao cinema, visitar um museu ou para comprar um livro, jornal ou revista.

Em segundo lugar, precisamos lembrar de situações em que o anonimato se coloca excepcionalmente como uma **proteção necessária para que críticas ou denúncias possam ser feitas**, seja para permitir o combate a crimes contra indivíduos, seja para viabilizar o combate a violações de direitos coletivos de grupos ou de toda a população.

Finalmente, é importante **separar conceitualmente o anonimato da prática de crimes em si**, até porque é normal que crimes não exijam a identificação prévia de seus autores. Para muitos

casos, a simples tipificação da conduta já inclui a ocultação da identidade do agente; para mais casos ainda, a exigência de identificação pode fragilizar a liberdade de expressão lícita, em todos os casos em que as pessoas se sintam vigiadas e, por isso, receosas em compartilhar suas histórias. Não por acaso, diversos artistas ao longo de toda a história se utilizaram de **pseudônimos e nomes coletivos para proteger sua identidade sem abrir mão de sua expressão cultural**.

Especificamente para a Internet, vale lembrar que todo computador sempre está identificado pelo menos por um IP, ainda que esse endereço possa não ser exclusivo.

8.2 Usos legais do anonimato no Brasil

As duas principais formas de proteção ao anonimato no Brasil são na proteção do sigilo da fonte jornalística e no uso difundido de denúncias anônimas em investigações do poder público.

8.2.1 Sigilo da fonte jornalística

O professor Walter Capanema, advogado e professor da Escola de Magistratura do Estado do Rio de Janeiro, cita os professores Vicente Paulo e Marco Alexandrino, em sua obra Direito Constitucional Descomplicado, para concluir que "não há conflito entre o art. 5o, IV, CF com a norma constitucional que garante o sigilo da fonte da informação (art. 5o, XIV: 'é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional')" *[CAPANEMA-2012]* (Página 109):

> Note-se que a garantia do sigilo da fonte não conflita com a vedação ao anonimato. O jornalista (ou o profissional que trabalhe com a divulgação de informações) veiculará a notícia em seu nome, e está sujeito a responder pelos eventuais danos indevidos que ela cause. Assim, embora a fonte possa ser sigilosa, a divulgação da informação não será feita de forma anônima, de tal sorte que não se frustra a eventual responsabilização de quem a tenha veiculado – e a finalidade da vedação ao anonimato é exatamente possibilitar a responsabilização da pessoa que ocasione danos em decorrência de manifestações indevidas. *[PAULO-ALEXANDRINO-2007]* (Página 112)

A advogada e especialista em direito penal Tatiana Moraes Cosate, em seu artigo "Liberdade de informação e sigilo da fonte", estabelece que "sem as fontes, seria praticamente impossível transmitir qualquer tipo de informação ao público, pois são elas que subministram os fatos e as informações ao repórter, sendo imprescindíveis na realização do trabalho jornalístico" *[COSATE-2009]* (Página 110).

No quarto capítulo, "Aspectos jurídicos do sigilo da fonte no Brasil", após lembrar decisões judiciais e posições de magistrados, Cosate conclui que "o entendimento pátrio é de que o sigilo da fonte configura-se como um direito absoluto, não existindo, no ordenamento jurídico, qualquer restrição ao uso desse direito".

Cosate cita a decisão do ministro Celso Mello no Supremo Tribunal Federal, em 1996, que "além de conferir ao jornalista o direito de não relatar a sua fonte de informação ou a pessoa

de seu informante em juízo, ela assegura e desautoriza qualquer medida tendente a pressionar ou a constranger o profissional da Imprensa a indicar a origem das informações a que teve acesso"*[COSATE-2009]* (Página 110):

> O ordenamento positivo brasileiro, na disciplina específica desse tema (Lei nº 5.250/67, art. 71), prescreve que nenhum jornalista poderá ser compelido a indicar o nome de seu informante ou a fonte de suas informações. Mais do que isso, esse profissional, ao exercer a prerrogativa em questão, não poderá sofrer qualquer sanção, direta ou indireta, motivada por seu silêncio ou por sua legítima recusa em responder às indagações que lhe sejam eventualmente dirigidas com o objetivo de romper o sigilo da fonte (...).
>
> Eis que - não custa insistir - os jornalistas, em tema de sigilo da fonte, não se expõem ao poder de indagação do Estado ou de seus agentes e não podem sofrer, por isso mesmo, em função do exercício dessa legítima prerrogativa constitucional, a imposição de qualquer sanção penal, civil ou administrativa." *[MELLO-STF-1996]* (Página 113)

Em outubro de 2015, então decano do STF, o ministro Celso Mello afirmou que o sigilo da fonte é o "meio essencial de plena realização do direito constitucional de informar", e "instrumento de concretização da própria liberdade de informação", em uma Reclamação ajuizada contra decisão de retirar uma reportagem do ar por conter fontes *em off* (no jargão jornalístico, sem serem identificadas). *[CONJUR-2016]* (Página 109)

8.2.2 Denúncias anônimas

Já no que se trata das denúncias anônimas, o professor Walter Capanema sustenta que a jurisprudência do Supremo Tribunal Federal admite a validade das denúncias "quando tais documentos forem produzidos pelo acusado, constituírem o corpo de delito, ou, ainda, quando a referida denúncia anônima for precedida de uma investigação para atestar a sua veracidade". Capanema continua: "Há julgados, inclusive, que ressaltam a importância da investigação policial deflagrada por denúncia anônima, pois o manto do anonimato tem servido como instrumento para a divulgação de condutas criminosas, especialmente através dos sistemas de 'disque-denúncia'." *[CAPANEMA-2012]* (Página 109)

O Disque Denúncia foi concebido no Rio de Janeiro em 1995, e registra mais de 2 milhões de denúncias acumuladas no estado desde então. A partir da experiência fluminense, o Disque Denúncia foi reproduzido em todos os estados e no distrito federal, e hoje conta com frentes especializadas em crimes ambientais, violência doméstica, criminosos foragidos e localização de pessoas desaparecidas.

Uma das missões é "manter a credibilidade e garantir a segurança ao seu denunciante através do anonimato" *[DISQUEDENUNCIA]* (Página 110). Segundo Zeca Borges, enquanto coordenador do serviço no Rio, em Recife e Campinas, falando para matéria do G1, a população prefere a denúncia anônima "porque teme um envolvimento com o caso". *[G1-2007]* (Página 111)

Ao longo dos últimos anos, órgãos públicos têm criado plataformas de denúncia online, como o NightAngel da Polícia Federal e o Web Denúncia, da Secretaria de Segurança Pública de São Paulo.

Veja também:

Tor e Rede Onion > *Rede Onion e Onion Web* > *Uma garantia técnica do anonimato* (Página 57)

8.3 Espaços anônimos e espaços vigiados

A Internet, por princípio e por construção coletiva, permite e encoraja o anonimato. Conforme a rede é adotada por processos comerciais e governamentais, é necessário garantir a segurança e a integridade destas comunicações e atividades online. As leis, regulamentações, padrões e protocolos relativos à rede devem preservar a possibilidade de criar e compartilhar conteúdo de forma aberta, irrestrita e sem permissão, tornando seguros, registrados e identificados tão somente as interações que concernem tais espaços comerciais ou governamentais.

A Constituição Brasileira de 1988, e seu art. 5º, veda o anonimato ao garantir a liberdade de expressão. O que essa vedação representa no meio digital, no entanto, se torna incerto à medida em que as tecnologias de informação e comunicação se integram às nossas atividades diárias, públicas e privadas, sem trazer consigo algumas garantias e direitos fundamentais que conquistamos na vida *offline*.

Em um passado não tão distante, todas as ações eram intrinsecamente *anônimas* – um grupo de pessoas conversando ou trabalhando juntas sabe quem falou e fez o quê, mas nenhum tipo de investida policial poderia descobrir, quiçá comprovar perante um tribunal, o que foi dito ou feito sem a cooperação de alguém de dentro ou algum tipo de mecanismo extremamente invasivo de vigilância (como uma escuta, infiltração ou patrulha policial). Toda ação deixa vestígios, mas para encontrá-los e entendê-los é necessário o trabalho especializado de detetives, e uma suspeita muito bem fundamentada de que algo errado havia ocorrido ali. Quase tudo o que acontecia ficava, a princípio, entre as testemunhas oculares.

Conforme as cidades cresceram em tamanho e população, instituições como bancos, cartórios, mercados, correios, fábricas e o próprio governo em uma posição vulnerável, ao ter que realizar transações sensíveis ou valiosas com pessoas que seus funcionários não conheciam pessoalmente.

Para estabelecer vínculos de confiança e oferecer defesa contra abuso e crimes foram criados vários mecanismos de identificação: cadastros de pessoas físicas e jurídicas, serviços de proteção aos comerciantes, bancos de dados bancários e de crédito, e outras formas das instituições

coletarem assinaturas, números de identificação e impressões digitais e poderem trocar ou conferir estas informações entre si.

A coleta de dados sobre indivíduos como etapa obrigatória para determinadas interações com clientes e cidadãos, serve tanto como meio de levar uma pessoa infratora à justiça quanto identificar que uma pessoa, vinda anônima das ruas, não é uma é uma impostora e sim a pessoa titular de uma conta bancária ou destinatária de uma encomenda.

Por princípio, a Internet reflete e amplifica o anonimato presente nas ruas e espaços públicos da cidade. Nos *chats*, fóruns e *blogs* e em muitas redes sociais, é possível se expressar e interagir a partir de um pseudônimo, um *nickname*, e facilmente trocá-lo para adquirir uma nova "identidade".

Conforme a Internet passa rapidamente de ferramenta de pesquisa e comunicação casual a parte integrada e dissociável da vida pública, das interações das pessoas com empresas e serviços governamentais, se torna ferramenta para roubar ou extorquir dinheiro, cometer estelionato e causar outros tipos de prejuízo. Com isso, torna-se necessário identificar, e possivelmente registrar, as atividades de uma pessoa dentro destes espaços sensíveis.

No entanto, a possibilidade de interação *online* de forma anônima e pseudônima fora destes espaços de apropriação da Internet pelos setores comerciais e governamentais que necessitam de controle e identificação é parte da concepção dos protocolos da rede, permitiu o fortalecimento de movimentos sociais e de uma maior participação política pelos cidadãos e cidadãs, fez surgirem novas formas de interação social, deu voz a incontáveis indivíduos e grupos marginalizados pelos meios de comunicação tradicionais, e sem dúvida foi um grande estímulo às inovações que *startups*, ONG's e pequenos empreendedores têm desenvolvido através da Internet, com notável participação do Brasil.

Nas palavras de David Kaye em relatório sobre criptografia e anonimato para as Nações Unidas: "anonimato online fornece a indivíduos e grupos uma zona de privacidade para manter opiniões e exercitar a liberdade de expressão sem interferência ou ataques arbitrários ou ilegais".

8.3.1 Proteção contra monitoramento

"Conforme nós lemos os jornais *online*, eles também nos lêem". O website Trackography, projeto do Tactical Tech Colletive para evidenciar as empresas que rastreiam a atividade de indivíduos na Internet para montar perfis de consumo e interesses para propaganda direcionada, ilustra bem esta frase.

Não só os jornais, mas quase todos os *websites* e aplicativos que utilizamos no dia-a-dia usam as informações que passamos a eles (como dados de localização, endereços de sites navegados e termos buscados) e todas as outras a que têm acesso (como detalhes de *hardware* dos nossos dispositivos, contatos e registros de chamadas) para montar o retrato mais fiel de seus usuários – os dados pessoais são "o combustível da economia da informação", como diz outra frase na ponta da língua dos *experts* em privacidade.

Tal proteção é uma ferramenta que deve estar disponível para todo o público, mas cujo interesse é ainda maior para crianças e adolescentes. Como salientou durante a CPI Pedro Affonso Hartung, conselheiro da sociedade civil do Conanda (Conselho Nacional dos Direitos da Criança e do Adolescente), há uma série de questões relativas à coleta, integração, monetarização e comercialização de dados pessoais, visando o direcionamento de publicidade.

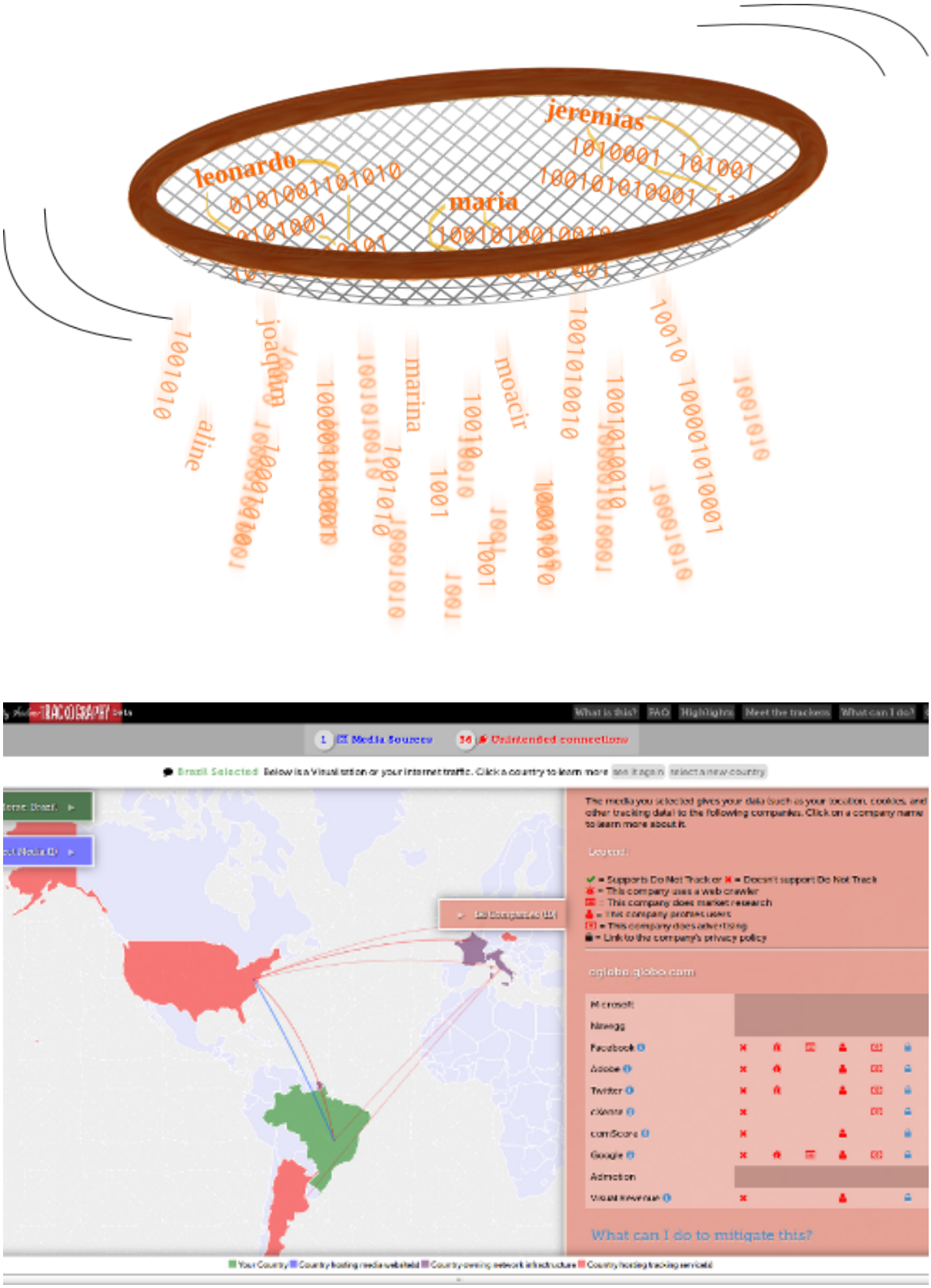


Fig. 8.1: Tela do Trackography mostrando as várias empresas, localizadas em diferentes países, que são acionadas quando se lê uma determinada matéria de um grande jornal brasileiro *online*.

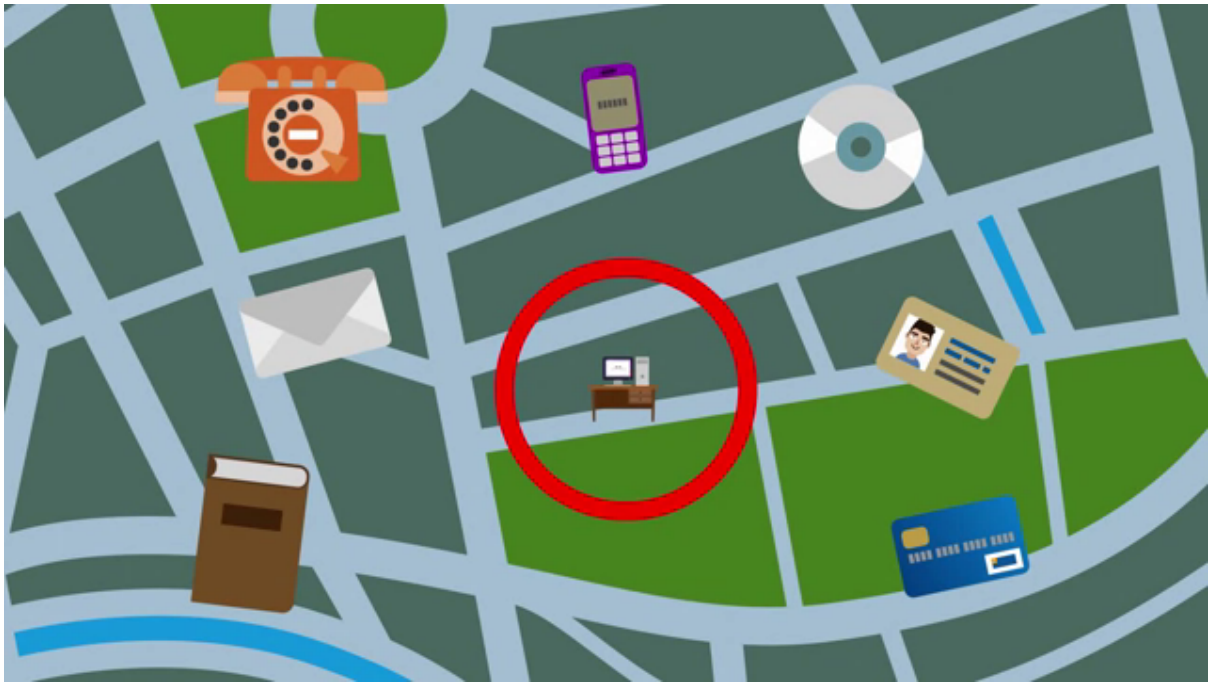
Violação da privacidade e proteção dados

- Violação ao direito à privacidade: aumento de armazenamento e integração de informações pessoalmente identificáveis;
- Motivos de segurança ≠ motivos econômicos
- Motivos econômicos: criação de *profiling* (criação de perfis) do *big data* para monetarização dos dados e comercialização das informações, visando o direcionamento de publicidade;
- Art. 7o, VIII, IX MCI: privacidade e proteção dos dados pessoais, cabendo ao usuário a concordância para coleta de dados. Criança pode aferir consentimento?
- Pesquisa do ano de 2013, realizada com jovens entre 09 e 23 anos, apontou que 26% não se importam com suas configurações de privacidade. Apontou também que dentre os dados pessoais compartilhados na rede, 60% afirmaram compartilhar fotos pessoais, 35% compartilham nome e sobrenome, outros 28% compartilham o nome da escola em que estudam, 10% chegam a compartilhar o número de celular enquanto 3,5% compartilham até o próprio endereço residencial139.
- PL 1746/2015 - Deputado Giovani Cherini (PDT/RS);

Crianças: público-alvo

- 40 milhões de crianças no Brasil;
- Crianças absorvem informações muito rápido;
- São receptoras e emissoras de informações;
- Estão formando seu raciocínio abstrato, e referenciam as marcas por meio de seriados, personagens, ídolos;
- **Triplo impacto**: são influenciadas, influenciam os responsáveis e são cativadas como futuros consumidores;
- Elo mais fraco da cadeia de consumo, mas responsável por sustentar vendas.

Neste cenário, há uma forte pressão da sociedade civil, de especialistas em tecnologia e do público em geral para diminuir a quantidade de dados transmitidos na rede e proteger os que são transmitidos com tecnologias de criptografia e de anonimização de dados.



As tecnologias de monitoramento *online* não são usadas somente por empresas. Após os vazamentos do ex-agente da CIA Edward Snowden de vários documentos internos da Agência de Segurança Nacional dos EUA (NSA), jornalistas começaram a relatar programa após programa onde a NSA e outras agências como a britânica GCHQ vigiam os principais cabos da Internet e permitem a analistas em seus quartéis (como outrora o próprio Edward Snowden) possam procurar e remontar todo o histórico de navegação e as comunicações de qualquer pessoa.

Tal busca é feita através de **selectors / seletores**. Um(a) analista pode pesquisar por atividades de um determinado endereço IP ou de e-mail, no tráfego que entra ou sai de um determinado país, ou somente das pessoas que visitaram um determinado website. Ao combinar seletores, é possível refinar a busca de forma muito poderosa.

Desde as primeiras revelações de vigilância, em junho de 2013, muito pouco foi feito para frear tal atividade por parte das agências de inteligência e seus parceiros internacionais. Uma reação positiva, no entanto, foi um forte movimento de desenvolvimento, ensino e simplificação de **tecnologias que impedem permitem navegar sem ser identificado(a)**. Ferramentas como o Tor e VPN's permitem usar a Internet através de servidores *proxy* ou de redes voluntárias de "desidentificação", de forma que a navegação na web se assemelhe mais a uma visita à biblioteca do que a um pedido de passaporte.

Veja também:

Tor e Rede Onion (Página 52)

Fig. 8.2: Em uma animação educativa do Projeto Tor, é explicado seu uso para proteger a navegação de monitoramento comercial, ao não expôr a localização nem detalhes do computador usado que possam identificar o(a) usuário(a).

8.3.2 Anonimização de dados

Outro campo onde o conceito de anonimato é não só bem-vindo como vital para a proteção das liberdades fundamentais é no processo de **anonimização** presente no **tratamento de dados pessoais**.

Com a rápida proliferação de sensores e pontos de coleta de dados, a crescente adoção de aplicativos e ferramentas *online* para interações sociais, políticas, comerciais e da vida pública, mais e mais bancos de dados são publicados e combinados com rastros digitais que guardam informações sensíveis sobre nossas vidas.

Há uma grande indústria das chamadas *data brokers*, empresas globais que compram e vendem dados sobre indivíduos para fins de segmentação de mercado. Tais repositórios corporativos de informação, quando aliados ao desenvolvimento de técnicas cada vez mais poderosas de cruzamento e mineração de dados, tornam cada vez mais fácil associar nossas ações em um determinado campo (compras no cartão, por exemplo) a ações em um campo completamente diferente (filmes favoritos).

Para evitar que informações em bancos de dados possam ser usadas sem identificar os indivíduos que geraram tais dados, é então aplicado um **processo de anonimização de dados**.

Legislações e regulamentações antigas de proteção de dados pessoais, como a HIPAA que regulamenta o tratamento de dados de saúde nos EUA e a Diretiva de Proteção de Dados Pessoais da União Europeia já reconhecem que procedimentos simples de anonimização – como a remoção de identificadores únicos como nomes e números de documento – conferem proteção aos dados armazenados.

A mera supressão de dados que identificam alguém diretamente, no entanto, não é o suficiente

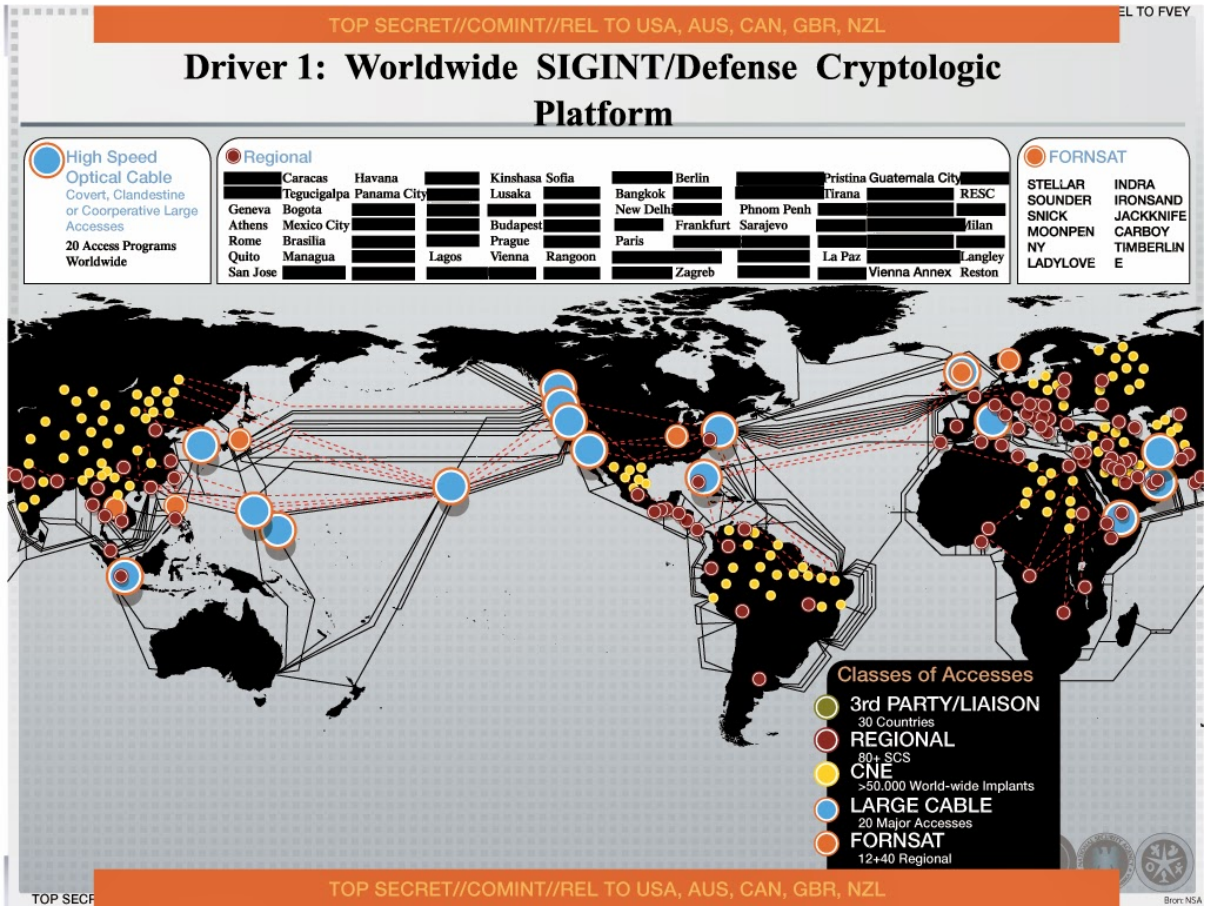
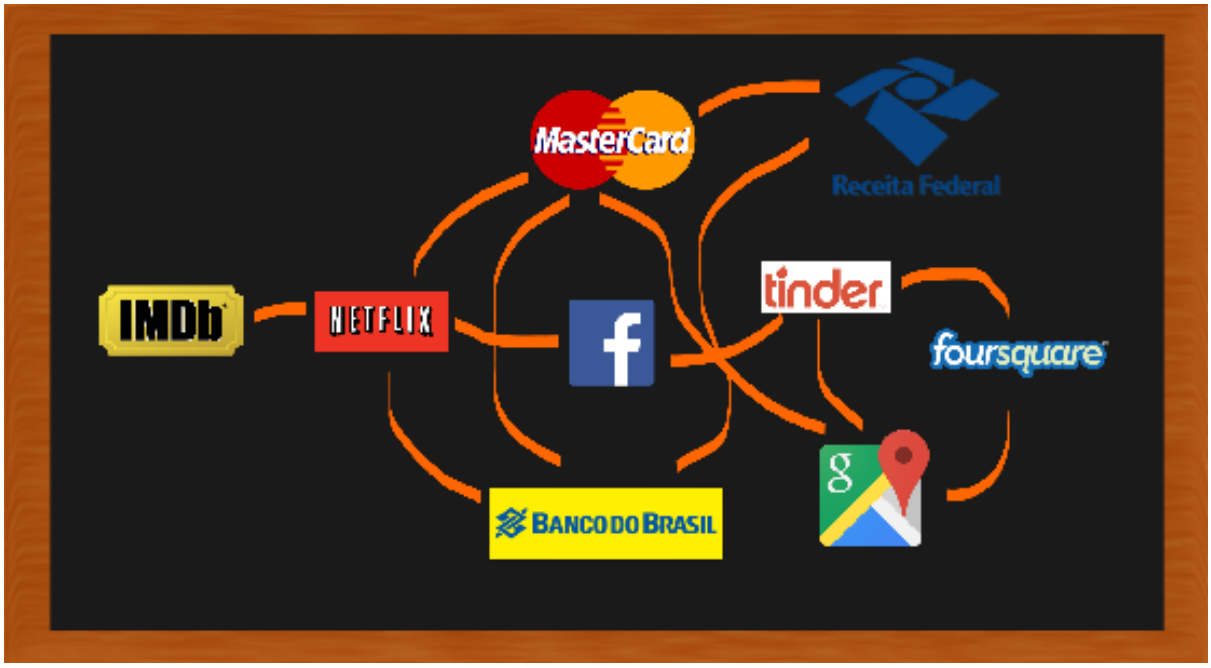


Fig. 8.3: Um mapa com os locais de interceptação de dados que a NSA possuía em 2012. Slide publicado em matéria do jornal holandês NRC Handelsblad



para impedir a "re-identificação" – dados aparentemente inócuos podem ser combinados para identificar uma pessoa. Um estudo clássico da pesquisadora Latanya Sweeney mostrou que é possível identificar pessoas unicamente com grande precisão sabendo-se somente o CEP, o gênero e a data de nascimento *[SWEENEY-2000]* (Página 114).

Textos legislativos mais atuais sobre proteção de dados levam em conta a maneira como os dados são anonimizados; tal processo deve possuir garantias técnicas de que os indivíduos que geraram os dados não podem ser re-identificados dado o estado da arte atual de técnicas de análise computacional.

8.4 ONU: proteção à privacidade, à criptografia e ao anonimato

Em junho de 2015, o Relator Especial em liberdade de expressão das Nações Unidas, David Kaye, publicou seu Report on encryption, anonymity and the human rights framework ("Relatório sobre criptografia, anonimato e o *framework* de direitos humanos").

O documento busca responder duas questões interligadas, segundo nota de lançamento do Conselho de Direitos Humanos da ONU: se os direitos à privacidade e à liberdade de opinião e expressão protegem o uso de ferramentas de criptografia e anonimato, e no caso positivo, como os governos podem impôr restrições a estas tecnologias respeitando o arcabouço legal de direitos humanos. David Kaye contou com a contribuição de 17 países e quase 30 organizações não-governamentais (como a Coding Rights, co-autora desta obra).

Em seu relatório, ele é enfático na proteção da criptografia e do anonimato como ferramentas para a promoção dos direitos humanos (tradução e grifos nossos):

> A respeito da criptografia e do anonimato, os Estados devem adotar políticas de não-restrição ou de proteção compreensiva, somente adotar restrições em casos es-

> pecíficos e atingindo objetivamente as demandas de legalidade, necessidade, proporcionalidade e legitimidade, exigir ordens judiciais para qualquer limitação específica, e promover a segurança e a privacidade online através da educação pública;
>
> **Leis nacionais devem reconhecer que indivíduos são livres para proteger a privacidade de suas comunicações digitais com o uso de tecnologias de criptografia e ferramentas que permitem o anonimato online**;
>
> Empresas, como os Estados, devem abster-se de bloquear ou limitar a transmissão de comunicações criptografadas e **permitir a comunicação anônima**. Atenção deve ser dada aos esforços para expandir a disponibilidade de *links* criptografados entre *datacenters*, apoiar tecnologias de segurança para websites e desenvolver criptografia fim-a-fim por padrão em larga escala. Atores do setor privado que provêem tecnologia para violar a criptografia e o anonimato devem ser especialmente transparentes quanto a seus produtos e clientes.
>
> O **uso de ferramentas de criptografia e anonimato** e uma melhor alfabetização digital **devem ser incentivados**. O Relator Especial, reconhecendo que **o valor de ferramentas de criptografia e anonimato depende de sua adoção em larga escala**, encoraja os Estados, organizações da sociedade civil e corporações a se engajar em uma campanha para trazer a criptografia por *design* e *default* para usuários(as) ao redor do mundo. *[KAYE-2015]* (Página 111)

Joana Varon, co-fundadora da Coding Rights, esteve durante a 29ª sessão do Conselho de Direitos Humanos da ONU, e relatou para o Boletim Antivigilância:

> Segundo Kaye, as discussões sobre encriptação e anonimato têm sido polarizadas no discurso sobre seu potencial uso criminal, mas que o debate precisa mudar para destacar também a proteção que a encriptação e o anonimato proporcionam, principalmente para grupos que vivem em situações de risco de interferências ilegais de suas comunicações. *[JOANA-ONU-2015]* (Página 116)

Segundo Joana, o relatório foi bem recebido pelo Brasil – que teve um envolvimento muito importante na defesa da privacidade na ONU, ao questionar junto com a Alemanha as práticas de vigilância em massa reveladas pelas primeiras matérias jornalísticas baseadas nos vazamentos de Edward Snowden. "Destaca-se da fala do Brasil, diante da apresentação do relatório: 'vemos valor em discutir a relevância de ferramentas de encriptação e anonimato para a proteção da privacidade e da liberdade de expressão e opinião de indivíduos"'.

8.5 Anonimato é legião, porque são muitos

Dados todos os novos nuances do conceito de "anonimato" trazidos pela Internet como espaço livre de comunicação e ao mesmo tempo espaço onde cada ação deixa rastros e onde a coleta e tratamento de dados é parte do modelo de negócios de grande parte das empresas, qualquer tentativa de entender e legislar sobre o comportamento *online* no que se refere à vedação constitucional ao anonimato deve entender que o conceito, à época da Assembleia Constituinte, representava apenas uma parcela dos significados que ele possui hoje em dia.

Kathleen A. Wallace publicou em 1999 uma análise chamada Anonymity ("Anonimato"), enquanto pesquisadora do Departamento de Filosofia da Universidade de Hofstra, de Nova York.

Wallace define o anonimato como **"a não-coordenabilidade de traços"** – ou seja, a dificuldade de associar dois ou mais rastros à mesma pessoa (tradução nossa):

> O anonimato é um tipo de relação entre uma pessoa anônima e outras, onde a primeira é conhecida somente através de um ou mais traços que não são coordenáveis com outros traços de modo a permitir a identificação da pessoa por inteiro. Considere um autor sem nome de um certo livro. Ela ou ele é desconhecida(o) dos outros – leitores, por exemplo – em alguns (mas não necessariamente todos) os aspectos; seu nome, suas relações familiares, seu endereço e etc. podem não ser conhecidos pelos leitores, mas o(a) autor(a) é conhecido(a) por ter escrito o tal livro. Então, se a descrição definitiva "autor(a) d'Os Versos do Capitão" não foi coordenada pelo público leitor com a pessoa chamada "Pablo Neruda", então o autor teria estado anônimo para tais pessoas (leitores) em alguns aspectos (sobrenome, endereço) em um determinado contexto (o público). O anonimato é sustentável à medida em que tal coordenação não pode ser feita (ou não sem um enorme esforço). *[WALLACE-ANON-1999]* (Página 116)

A autora segue definindo melhor sua teoria – cujos propósitos ou objetivos podem ser divididos em três gandes categorias:

- *Agent anonymity, ou "anonimato do agente"*, com o objetivo de perpetuar as ações da pessoa anônima. Aqui, Wallace dá o exemplo de doadores e compradores, autores, fontes jornalísticas e pessoas que desejam fazer denúncias de forma anônima, além do Unabomber, indivíduo que enviava bombas para cientistas da computação de forma anônima.
- *Recipient anonymity, ou "anonimato do receptor"*, com o objetivo de prevenir ou proteger a pessoa anônima de reações. Wallace cita pessoas que se submetem a testes de HIV e outras condições de saúde estigmatizador.
- *Process anonymity, ou anonimato do processo*, com o objetivo de manter em curso algum processo. Nesta categoria entram testes duplo-cego e revisões científicas, o anonimato em pesquisas, reportagens jornalísticas e em processos judiciais como forma de manter a imparcialidade ou neutralidade de processos – o conhecido "véu da ignorância".

Em um ensaio posterior, de 2008, para a o livro The Handbook of Information and Computer Ethics ("o livro de mão da ética da informação e dos computadores"), Kathleen A. Wallace desenvolve mais como o anonimato "pode ser exercido de diversas maneiras e que há diversos propósitos, tanto positivos quanto negativos, para os quais o anonimato pode servir, como, positivamente, promover a liberdade de expressão e a troca de ideias, ou proteger alguém de tornar-se público de forma indesejada, ou, negativamente, discursos de ódio sem responsabilização, fraudes e outras atividades criminosas" *[WALLACE-ANON-2008]* (Página 116).

Wallace também reconhece que "o anonimato e a privacidade são considerados como fortemente relacionados, sendo o anonimato uma das maneiras de garantir a privacidade". Entre algumas das questões onde o anonimato se apresenta como solução, ela cita **proteção contra técnicas de data mining e monitoramento** ("ao estabelecer os padrões de preferências de um(a) consumidor(a), publicitários podem fazer propagandas seletivas ou fazer sugestões para compras que são consistentes com os caminhos de interesse expressados pelo(a) usuário(a) ou por seus padrões de compras") e a **liberdade de expressão** ("uma função do anonimato pode ser permitir que um indivíduo aja ou se expresse de maneiras que não seriam possíveis ou reconhecidas se a identidade do indivíduo fosse conhecida. Por exemplo, uma escritora mulher

usar um pseudônimo masculino [aqui, um pseudônimo pode de fato funcionar para garantir o anonimato] pode garantir o reconhecimento de seu trabalho que de outra maneira não teria nem ao menos sido publicado").

Na conclusão da obra, Kathleen A. Wallace despreza legislações que tratem o anonimato de modo simplista:

> Como há muitas formas de comunicações e atividades anônimas, e uma variedade de propósitos para as quais o anonimato pode servir, pode ser importante distinguir que tipo de comunicação ou atividade está envolvido, em vez de ter uma única política legislativa ou posição ética sobre o anonimato (Allen, 1999 ["Internet anonymity in contexts"]).

8.6 Por uma reinterpretação do anonimato

Especificamente no Brasil, uma tentativa interessante de reconciliar a vedação constitucional ao anonimato em publicações com seu papel vital para a manutenção da liberdade de expressão garantida pela própria Constituição é a do professor Walter Capanema, advogado e professor da Escola de Magistratura do Estado do Rio de Janeiro. Em seu ensaio O Direito ao Anonimato, Capanema pede uma "nova interpretação do anonimato" no Brasil após rever o arcabouço legal brasileiro sobre o tema e analisar seu uso corrente na Internet:

> Muito embora a literalidade do art. 5º, IV da Constituição Federal proíba o anonimato, tendo em vista a importância que esse instituto é para a salvaguarda da identidade, vida, liberdade e honra do indivíduo, propõe-se uma reinterpretação dessa norma em consonância com a própria liberdade de expressão, de modo a afirmar que o anonimato vedado pela Carta Magna é só aquele que cause prejuízos a terceiros.
>
> O anonimato, sem dúvida alguma é um escudo contra a tirania, de onde quer que ela surja.
>
> [...]
>
> A Constituição Federal, ao vedar o anonimato, estabeleceu a presunção de que a manifestação de vontade anônima só iria ser utilizada para causar prejuízos a terceiros e, com isso, estabeleceu uma proibição geral, ao invés de permiti-la em situações específicas.
>
> Não se deve admitir o anonimato como instrumento para a prática de crimes, especialmente os contra a honra, nem para atos que causem danos morais e materiais a terceiros.
>
> A proteção à identidade do indivíduo através do anonimato deverá ser consagrada em situações as quais as doações anônimas à caridade e a decorrente de cultos religiosos; denúncias de crimes, especialmente os políticos, grupos de auto-ajuda (Narcóticos Anônimos e Alcoólicos Anônimos, pessoas que sofreram abusos sexuais, pessoas com algum distúrbio ou doença e que não querem revelar a identidade).
>
> O anonimato deve ser admitido como um instrumento para a efetivação da liberdade de expressão, de modo a impedir ou evitar efeitos danos ao emitente da von-

tade.

Portanto, propõe-se a reinterpretar o art. 5º, IV, CF, de forma a estabelecer que o anonimato ali vedado é apenas para as declarações de vontade que possam causar prejuízos a terceiros. *[CAPANEMA-2012]* (Página 109)

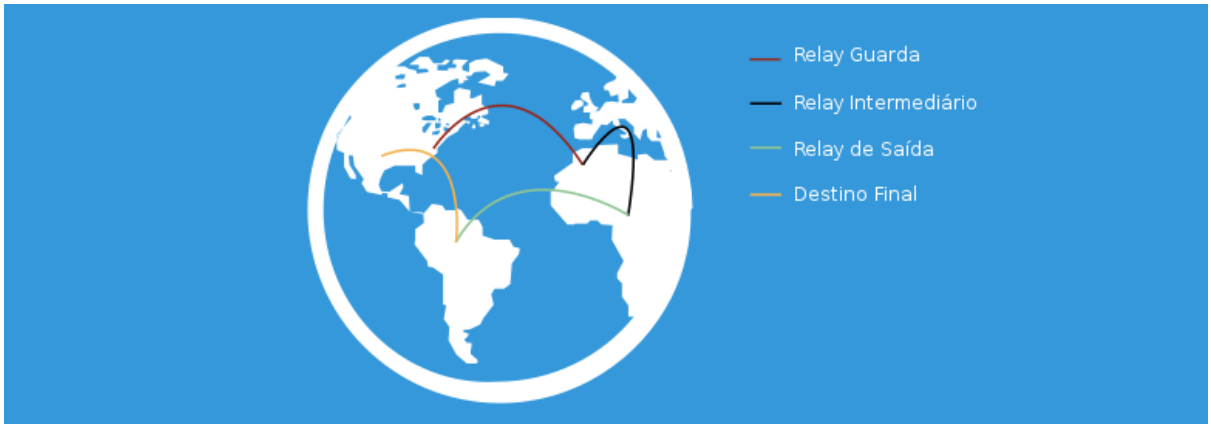
CAPÍTULO 9

Tor e Rede Onion

Talvez o ponto de maior preocupação mas também menor familiaridade da CPICIBER seja o uso do Tor. Aqui, apresentamos uma breve história do Tor e de como ele funciona (tanto para pessoas não serem associadas à sua navegação quanto para hospedar sites e serviços que não podem ser localizados), as ocorrências e tentativas passadas de quebrar o anonimato que a rede Tor provê, e a nossa posição sobre que métodos devem ser utilizados para investigar crimes na chamada "dark web", que preferimos chamar de **onion web**. Esta rede também frequentemente é chamada de *deep web*, um termo que já possui outro significado e que explicamos melhor na seção "Dark Web? Deep Web?" abaixo.

9.1 Tor

O Tor – nome derivado do antigo acrônimo "The Onion Routing", "O Roteamento Cebola" – é o nome tanto de um software mantido por uma organização sem fins lucrativos sediada em Massachussetts, EUA, quanto da rede mundial de *relays* ("retransmissores"), computadores mantidos por pessoas e organizações voluntárias.



9.1.1 Como funciona

Quando alguém usa o Tor para acessar um site ou ler e-mails, seu computador escolhe três desses relays para encaminharem seu tráfego de forma que ele saia para a Internet com o IP do

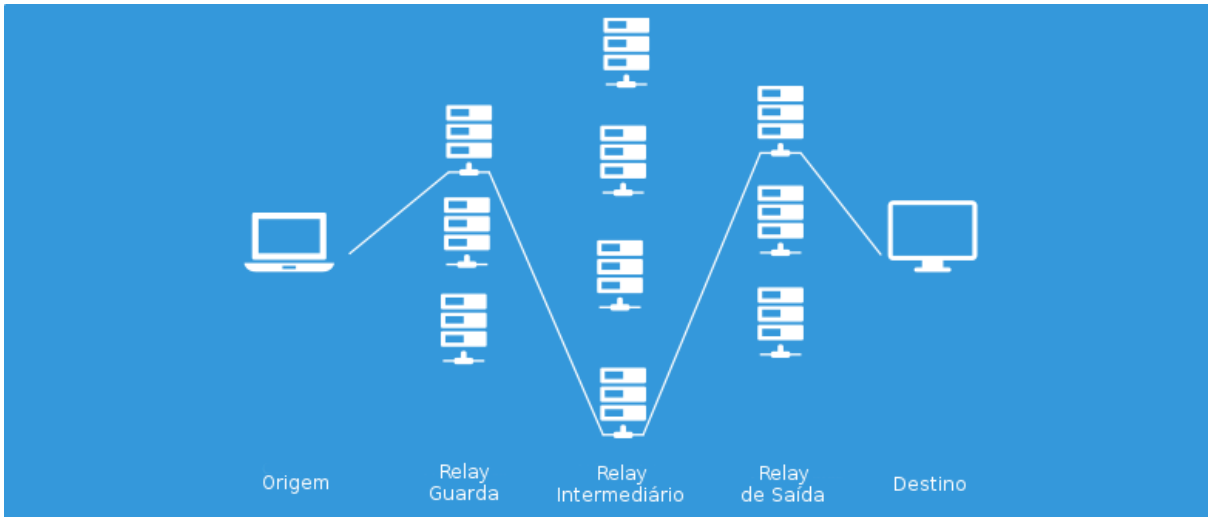


Fig. 9.1: Imagens traduzidas do guia "How Tor Works?" de Jordan Wright *[WRIGHT-TOR-2015]* (Página 116). Licença: CC BY 3.0 <https://creativecommons.org/licenses/by/3.0/>.

último deles, o *relay* de saída.

Como há muitos *relays* na rede Tor (cerca de 7200 em 15 de fevereiro de 2016), e pessoas utilizando o serviço em todo o mundo (mais de 2 milhões na mesma data), usá-la tem o efeito de anonimizar a sua conexão, impedindo que os seus pacotes de dados trafegados sejam ligados ao seu endereço IP tanto pelo provedor de conexão quanto pelo servidor acessado.

Além disso, quando o computador vai enviar uma mensagem ou acessar uma página através da rede Tor, o conteúdo é enviado com três camadas de criptografia, uma para cada *relay*. Isto e mais algumas técnicas matemáticas garantem que nem mesmo os *relays* que participam da rede possam saber o que estão encaminhando e ao mesmo tempo quem é o remetente.

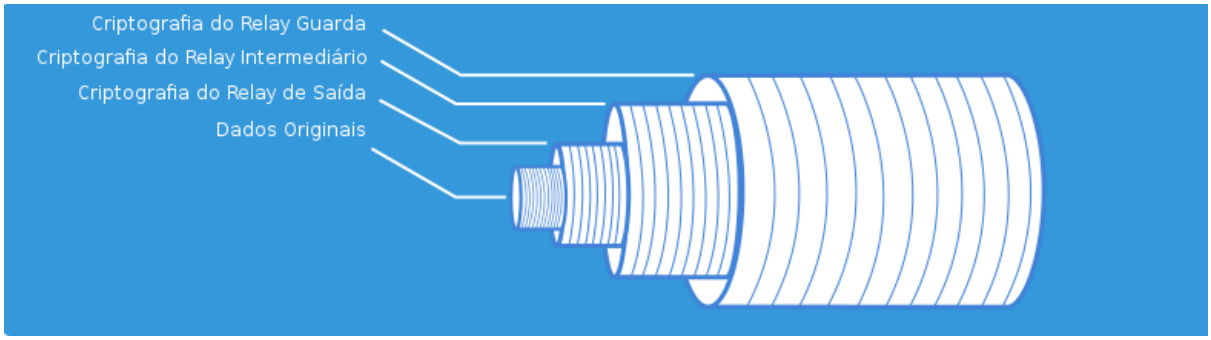


Fig. 9.2: Imagem traduzida do guia "How Tor Works?" de Jordan Wright *[WRIGHT-TOR-2015]* (Página 116). Licença: CC BY 3.0 <https://creativecommons.org/licenses/by/3.0/>.

O *relay* guarda, primeiro da fila, pode saber que determinado IP usou a rede Tor, mas não sabe para quê. O *relay* intermediário não tem acesso nem ao conteúdo, nem ao remetente, nem ao destinatário. O *relay* de saída finalmente encaminha o pacote para a "Internet aberta", então deve saber o destinatário e o conteúdo, mas não o remetente. Se há uso de criptografia entre remetente e destinatário (o que grande parte dos serviços na Internet têm empregado), o *relay* de saída também não consegue saber o conteúdo do acesso ou da comunicação.

Veja também:

Criptografia (Página 25)

A tecnologia principal por trás do Tor, o "roteamento cebola" (nome dado devido às camadas de criptografia sobrepostas), tem suas origens no Laboratório de Pesquisa Naval dos EUA. Paul Syverson, um matemático da equipe, diz que a ideia "não é prover comunicações anônimas, mas sim separar a identificação do roteamento". Através de técnicas de criptografia, e tendo pessoas diversas o suficiente e espalhadas pelo mundo dispostas a manter *relays*, a Rede Tor funciona como uma comunidade voluntária que acredita que "o uso de uma rede pública não deve automaticamente revela as identidades das partes que se comunicam" *[SYVERSON-2011]* (Página 114). Para Jacob Appelbaum, pesquisador de segurança, desenvolvedor e porta-voz do Projeto Tor, a rede tem o objetivo de "instrumentalizar a liberdade de conexão", um dos princípios da Internet.

Após o laboratório tornar o código do software público em 2004 e ser fundada a ONG Tor Project para mantê-lo de forma independente em 2006, o tamanho da rede de *relays* cresceu bastante, tanto através de voluntários(as) individuais quanto de variadas entidades que defendem a liberdade de expressão: organizações sem fins lucrativos como as americanas Mozilla e Access Now e a alemã Torservers.net; universidades como a de Galileo, na Guatemala, e as de Michigan e Pennsylvania nos EUA; a biblioteca Lebanon, em New Hampshire, EUA, e até galerias que abrigam o projeto artístico Autonomy Cube, como a Casa Edith Russ na Alemanha.

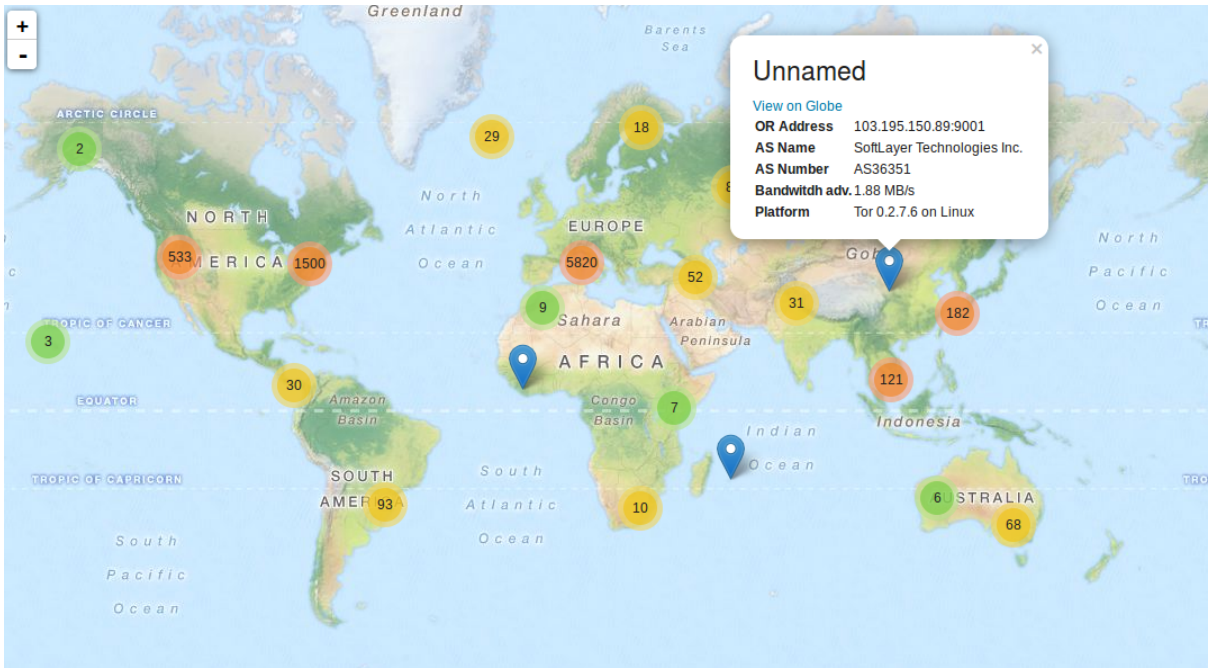


Fig. 9.3: Visão geral dos *relays* Tor ao redor do mundo, agrupado por regiões de proximidade. Imagem retirada do site `map.torservers.net`, em dezembro de 2015.

O Tor é uma ferramenta muito importante para uma variedade de profissões e atividades ao proteger as comunicações e a navegação online. Tanto jornalistas investigativos quanto policiais e agentes de inteligência usam o Navegador Tor para conduzir suas investigações sem alertar os sites investigados sobre suas visitas; ativistas e defensores de direitos humanos usam a ferramenta para se organizar e discutir temas controversos sem risco de represálias, prisão ou morte em regimes não-democráticos (como no Irã, na China e na Síria). Através de ferramentas

Fig. 9.4: Parte dos membros pagos e voluntários do Projeto Tor, em um vídeo de agradecimento ao agregador social de notícias Reddit, que dividiu 10% de seu lucro em doações para projetos e organizações votados pelos(as) usuários(as). O Projeto Tor foi um deles, e recebeu US$ 82 mil.

de chat que usam a rede Tor como o Tor Messenger e o Ricochet, jornalistas e advogados podem conversar de forma segura com suas fontes / clientes sem gerar trilhas de informação que possam levar terceiros à identidade ou à localização dos últimos *[ANTIVIG-CHATANONIMO-2015]* (Página 114).

Milhões de cidadãos e cidadãs "comuns" usam o Tor para navegar pela Web sem serem monitorados por trackers, que usam o endereço IP, cookies e outras tecnologias de rastreamento para enxergar perfis de comportamento e consumo e gerar propagandas direcionadas *[ANTIVIG-TRACKERS-2015]* (Página 114), escapar de sistemas de vigilância em massa conduzida por agências de inteligência ou buscar informações e cuidado em temas pessoais e sensíveis como problemas de saúde, alcoolismo, traumas por exploração sexual ou psicológica, etc.

9.1.2 À prova de censura: o Tor é feito para não poder ser bloqueado

O Tor também é usado para evadir barreiras de censura, como o bloqueio de redes sociais, serviços de comunicação e sites políticos em países como o Irã e a China, que desde 2009 bloqueia o acesso aos *relays* da rede Tor em seus provedores (os endereços IP dos *relays* são públicos). A resposta a isso foi o desenvolvimento das *bridges* ("pontes"), *relays* guarda que não são listados publicamente e que o projeto Tor distribui de maneira privada, em pequenas quantidades, através de e-mail.

O consequente emprego de técnicas de *deep packet inspection* ("inspeção profunda de pacotes") para identificar os pacotes de conexão com as bridges e bloqueá-los (uma prática extremamente

intrusiva, que no Brasil violaria o Marco Civil da Internet tanto em seu art. 7º, inciso II, relativo à inviolabilidade das comunicações, quanto em seu artigo 9º, relativo à neutralidade da rede) foi contornado com a criação dos *pluggable transports*, ferramentas que camuflam o tráfego entre a pessoa e a bridge para que se pareça com o de outra aplicação (por exemplo, uma ligação via Skype ou o envio de um e-mail).

9.2 Rede Onion e Onion Web

Até agora, vimos como o Tor permite às pessoas acessar conteúdos e se comunicar na Internet sem que suas atividades deixem registros que possam lhes identificar. Outra funcionalidade do Tor é permitir a criação de "serviços escondidos" (hidden services), ou "serviços *onion* / cebola" (onion services). Eles formam o que é conhecido como "rede onion", "dark web", ou (erroneamente, como veremos abaixo) "deep web".

Quando se opera um site na *onion web*, ele passa a ser acessível através da rede Tor com um endereço especial, como `as2xfiuknfagm53d.onion`. Ele permite à rede de *relays* estabelecer um canal de comunicação onde tanto o computador cliente (quem acessa) quanto o computador servidor (o site acessado) desconhecem o endereço IP ou qualquer outro dado que possa ser associado à localização ou à identidade das pessoas que os operam.

O objetivo dos serviços *onion*, como publicado no blog do projeto, é "prover uma maneira de usuários(as) do Tor criarem sites e serviços acessíveis exclusivamente dentro da rede Tor, com características de privacidade e segurança que os tornam úteis e atraentes para uma ampla variedade de aplicações".

Estas "características de privacidade e segurança" de fato vão muito além de esconder a localização do servidor – segundo Roger Dingledine, fundador do Projeto Tor e idealizador dos serviços *onion*, eles provêem autoautenticação (isto é, o próprio endereço do site pode ser usado

para autenticá-lo como verdadeiro e não um site falso se passando por ele), criptografia fim-a-fim (isto é, a garantia da confidencialidade das comunicações entre as duas partes), *NAT punching* (uma forma de hospedar sites e serviços em redes compartilhadas ou atrás de *firewalls*) e área de superfície delimitada (um modo simples de expôr somente as portas necessárias do servidor, desvinculadas de seu endereço IP).

Em outubro de 2014, o Facebook passou a manter um serviço *onion*, no endereço `facebookcorewwwi.onion`, como forma de tornar as conexões via Tor de seus usuários mais seguras e eficientes. Isto foi feito não para esconder sua localização – a Facebook Inc. é uma empresa formalmente estabelecida, e os locais de seus *datacenters* conhecidos – mas para ser acessível a pessoas em países onde a rede social é bloqueada, como na China e na Turquia, e por usuários que se sentem confortáveis em ceder ao Facebook suas informações sociais, mas não seu endereço IP ou localização.

9.2.1 Uma garantia técnica do anonimato

Operar um serviço *onion* é o meio técnico mais confiável de garantir de fato a promessa de anonimato em uma denúncia – projetos como o GlobaLeaks e o SecureDrop fornecem software livre e gratuito para criar canais de denúncia anônima na imprensa e em empresas. Por serem acessíveis somente através da rede Tor, eles colhem as informações de denúncia sem deixar rastros não-intencionais que possam levar à/ao denunciante; como não é necessário encaminhar o tráfego para a Internet "aberta", todo o caminho entre denunciante e servidor é protegido de espionagem ou censura.

Algumas organizações que usam esta tecnologia são os jornais Washington Post, Guardian e New Yorker; a revista Forbes; e a ONG Greenpeace. Outros canais de denúncia surgiram focados especificamente no combate à corrução, como o Allerta Anticorruzione na Itália, o OCCRPLeaks na Bósnia, o Brussel Leaks na Bélgica, o Xabardocs na Ucrânia e o InfodioLeaks na Venezuela.

Já o WildLeaks usa a rede Tor para receber denúncias relacionadas "à vida selvagem e aos delitos florestais". Em vez de encarar diretamente criminosos armados, o projeto da ONG Elephant Action League "quer mirar os maiores traficantes de chifres de rinocerontes e presas de elefantes, que lucram milhões de dólares com sua atividade", segundo matéria da National Geographic Brasil *[NATGEOBR-WILDLEAKS-2014]* (Página 112). Algumas das 24 ocorrências recebidas durante os três primeiros meses de operação, em 2014, foram denúncias "de caça a tigres no norte de Sumatra, de contrabando de macacos, em particular chimpanzés, na África Central, atividades madeireiras ilegais no México, Malawi e Rússia, [e] pesca ilegal na costa do Alasca."

Veja também:

Anonimato Online > Usos legais do anonimato no Brasil > Denúncias anônimas (Página 39)

9.2.2 A censura à rede fere a liberdade de conexão

O que torna o bloqueio ou a censura automática de conteúdo (como pornografia infantil e crimes de ódio) incompatível com o princípio da *liberdade de conexão*, embutido nos protocolos da Internet e materializado aqui pelo Tor, é que qualquer mecanismo técnico que possibilite tal

censura será inevitavelmente explorado por indivíduos ou organizações com fins não tão nobres quanto o da proteção das pessoas e a investigação de crimes. Como disse Jacob Appelbaum, pesquisador de segurança e membro do Projeto Tor, ao responder um oficial da polícia alemã "se era possível bloquear determinados conteúdo abusivos da *onion web*", num painel do evento re:publica 2015:

> Nós não podemos censurar este conteúdo [pornografia infantil e venda de armas] porque a natureza da liberdade de conexão significa que se pusermos uma pessoa no meio para policiar o conteúdo, vários tipos diferentes de conteúdo ficarão fundamentalmente em risco; por exemplo há esta questão bastante importante e séria – eu levo bem a sério. O genocídio tibetano, perpretado pelo governo Chinês, é um assunto que tal governo gostaria de censurar, para eles é um assunto muito tabu. Se nós embutirmos a censura tecnologicamente nos nossos sistemas, as máquinas simplesmente farão valer a censura indiscriminadamente para quem quer que controle essas tecnologias, [...] como você sabe que aconteceu com a lista de censura aqui [na Alemanha], e de fato com vários exemplos históricos de vigilância e censura. Fundamentalmente, a solução não é mais vigilância e mais censura, e sim enfrentar o núcleo, a raiz do problema.

Veja também:

Questões Emergentes > Deep Web (Página 76)

9.3 Quebras da Rede Onion em investigações policiais

Dentre as operações policiais passadas a usuários(as) do Tor e operadores(as) de sites na *onion web* ao redor do mundo, relativamente poucas foram através de ataques técnicos. Apresentamos aqui alguns detalhes sobre os métodos mais relevantes – em um caso, uma falha no funcionamento interno da rede Tor; no outro, a exploração de falhas de segurança nos servidores dos sites. Então discutimos os limites e os riscos desse tipo de abordagem, e apresentamos outras mais saudáveis para a manutenção das liberdades na Internet, da privacidade e dos direitos humanos, e também mais dentro da realidade técnica e financeira da grande maioria das investigações.

Durante a investigação conduzida pelo FBI sobre o Silk Road 2 (um mercado onde vendedores(as) podiam anunciar, se comunciar com clientes e fazer as transações sob um pseudônimo, bastante conhecido pela oferta de narcóticos e substâncias psicoativas), foi citada uma infiltração na rede *onion* que permitia descobrir o endereço IP verdadeiro de um site disponível nesta rede. O Projeto Tor atualizou o software para que não permitisse mais tal ataque em julho de 2014, ao descobrir e anunciar a atividade anômala na rede, que perdurou por seis meses. Através de um novo documento anexado a um dos processos judiciais do Silk Road, foi descoberto que o FBI foi ajudado por um "instituto de pesquisa sediado em uma universidade".

O período de duração da vulnerabilidade e outras evidências apontam para o trabalho de um time de pesquisadores da universidade americana Carnegie Mellon *[WIRED-SR2-2015]* (Página 109). Roger Dingledine, fundador do Projeto Tor, afirmou que a universidade recebeu 1 milhão de dólares para conduzir a pesquisa *[OLHARDIGITAL-TORCMU-2015]* (Página 111).

Outro modo utilizado para identificar o verdadeiro IP dos sites na rede *onion*, em operações

policiais ou ações judiciais, é a invasão direta do servidor – aproveitando-se de erros de configuração de quem opera o site, ou vulnerabilidades nos softwares utilizados por ele. Através destas técnicas – combinadas com a investigação "tradicional", sem quebras de sigilo, online e offline – o FBI conduziu a operação que prendeu Ross Ulbricht, acusado de operar o "primeiro" Silk Road.

Utilizar vulnerabilidades de segurança, no entanto, tem um custo alto e traz uma série de responsabilidades e riscos.

Veja também:

Questões Emergentes > Invasão de computadores (Página 81)

Os métodos da Operação Darknet, que prendeu pelo menos 55 pessoas no Brasil envolvidas com troca de imagens de pornografia infantil na rede *onion*, são desconhecidos. O coordenador da operação, Rafael França, diz para a VICE News que sua equipe conseguiu identificar dezenas de usuários(as) da rede que compartilhavam pornografia infantil, utilizando "ferramentas desenvolvidas e metodologias inéditas de pesquisa" *[VICE-DARKNET-2014]* (Página 111).

É possível que tenha havido uma colaboração com o FBI – as prisões da operação brasileira foram feitas três meses após o Projeto Tor consertar a brecha que permitia o ataque de identificação usado pela agência, mas a vulnerabilidade era voltada a identificar os servidores dos sites (como um fórum de troca de imagens) e não quem os acessava (seus endereços IP permaneceriam ocultos) *[BRASIL-DARKNET-2014]* (Página 109).

O uso de tal método também desperta algumas questões idênticas às do seu uso no Silk Road 2: ele não pode ser direcionado a um site específico, envolvendo necessariamente a quebra da proteção das centenas ou milhares de sites e serviços legítimos operando na rede. Se esse tipo de abordagem desperta uma série de dúvidas até em situações extremas, certamente não deve ser a abordagem corriqueira para investigar crimes na *onion web*.

Outros métodos mais "tradicionais" também foram usados com sucesso na Operação Darknet, como mapear websites em espaços e meios públicos ("open source intelligence") e infiltrar agentes. O coordenador Rafael França explica, na mesma matéria da VICE News: "Nós descobrimos e fizemos contato com comunidades para pessoas interessadas em pornografia infantil, e gradualmente começamos a nos comunicar com elas".

Apesar da localização dos websites não poder ser descoberta quando ele opera dentro da rede Tor, ainda é necessário tornar seus endereços de acesso públicos para potenciais clientes, então um mínimo de exposição é necessário: seja em um site que os catalogue manualmente como a Hidden Wiki, (um tipo de Wikipédia para sites conhecidos na *onion web*) através de fóruns na Web aberta, ou outros meios.

É possível então analisar estes meios sistematicamente para criar listas de websites e analisar fóruns e canais públicos como o Reddit e o Pastebin, para criar buscadores análogos ao Google e Bing e conduzir análises específicas de combate a determinados crimes.

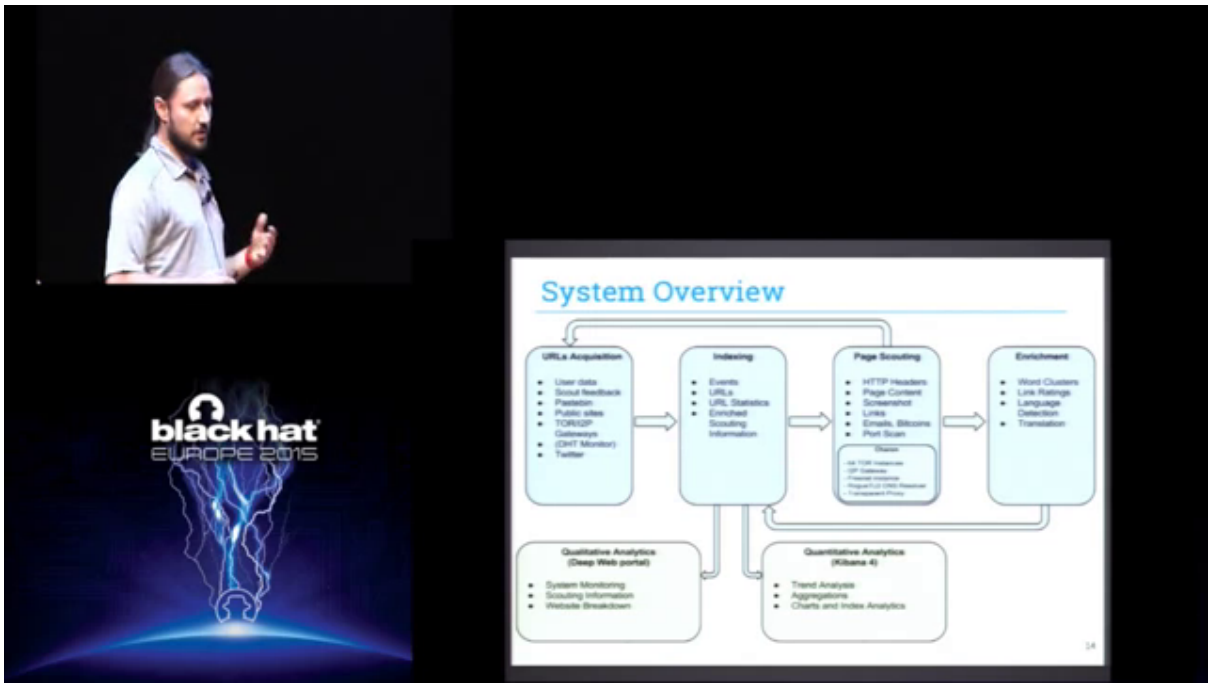


Fig. 9.5: Os pesquisadores Marco Balduzzi e Vincenzo Ciancaglini apresentaram a pesquisa em ferramentas de investigação para a Deep Web que desenvolveram através de análise de dados disponíveis publicamente, sem quebras de sigilo, na apresentação Cybercrime in the Deep Web.

CAPÍTULO 10

Segurança Cibernética

10.1 Definição

O conceito de **segurança cibernética** é difuso; assim como conceitos semelhantes de 'segurança da informação', 'ciberguerra' e 'cibervigilância', eles "não foram acordados através de um órgão internacional mediante um acordo vinculante, ou emitindo um documento que determine padrões" *[ROSSINI-CIBERSEG-2015]* (Página 113)

De acordo com a UIT / ITU (União Internacional das Comunicações, um órgão da ONU), a segurança cibernética é "a coleção de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, orientações, abordagens de gestão de risco, ações, treinamentos, melhores práticas, seguros e tecnologias que podem ser usados para proteger o ambiente cibernético, a organização e propriedades de usuários(as). A organização e as propriedades incluem dispositivos de computação conectados, funcionários(as) e colaboradores(as), infraestrutura, aplicativos, serviços, sistemas de telecomunicações e a totalidade de informação transmitida e/ou armazenada no ambiente cibernético. A segurança cibernética busca garantir a obtenção e a manutenção das propriedades de segurança da organização e das propriedades do(as) usuários(as) contra riscos de segurança relevantes no ambiente cibernético" *[ITU-CIBERSEG-2008]* (Página 115)

A União Europeia define o conceito como o conjunto de "salvaguardas e ações que se podem empregar para proteger o domínio cibernético, tanto no âmbito civil quanto militar, frente às ameaças vinculadas com suas redes interdependentes e sua infraestrutura de informação, ou que possam afetar a estas". *[EC-CIBERSEG-2013]* (Página 110)

Já o governo brasileiro, através do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), define a segurança cibernética como "a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas" *[BRASIL-CIBERSEG-2015]* (Página 109).

Abordagens ruins da segurança cibernética e de como se proteger de ameaças digitais podem gerar tanto sistemas de vigilância em massa – como os documentos vazados por Edward Snowden revelaram ser o caso por parte de agências de intleigência dos EUA, da Inglaterra e de países aliados e, pode-se argumentar, também o da *retenção de dados do Marco Civil da Internet* (Página 18) – quanto por censura e perseguição de pesquisadores de segurança (como na China) e uma excessiva aparelhagem ofensiva de "guerra cibernética" (outro conceito difuso)

Como escrevem Andrew Puddephatt e Lea Kaspar, *experts* em política e governança da Internet da Global Partners Digital, para a openDemocracy:

> Entre a sociedade icvil e grupos de interesse público, no entanto, ainda há no momento pouco engajamento ou mesmo pesquisa sobre este assunto [da segurança cibernética] – algo que desbalanceia o debate e insere a segurança cibernética como algo para os sistemas, em vez de para as pessoas. Mas a segurança cibernética é intrinsecamente sobre pessoas. Como uma área da política interessada na regulamentação do comportamento *online*, o modo como ela é definida implementada terá – e já está tendo – implicações profundas para direitos humanos essenciais como a privacidade e a liberdade de expressão.
>
> [...] Acima de tudo, precismaos lutar por uma abordagem aberta, inclusiva e multissetorial da elaboração de políticas. Em uma sociedade democrática, a implementação da segurança cibenrética demanda o consentimento informado da população – o que significa garantir que vozes fora das agências de segurança estejam envolvidas no debate.
>
> [...] A segurança cibernética é uma questão que chega na própria essência do que é a internet. A internet nunca foi, no fim das contas, feita para ser segura – por design ela é interoperável, multijurisdicional e horizontal, qualidades que raramente conduzem à segurança. Mas são estas qualidades que a tornam valiosa e fazem valer a pena lutar por ela. Se queremos que ela continue desta maneira, esse é um debate que não podemos nos dar o luxo de evitar. *[PUDDEPHATT-KASPAR-CIBERSEG-2015]* (Página 113)

10.2 Brasil

No Brasil, as principais estruturas de segurança cibernética são o os órgãos de inteligência e defesa cibernética, ligados ao Ministério da Defesa e ao GSI/PR (CDCiber, Abin), a Polícia Federal, e os grupos de tratamento de incidentes de segurança brasileiros – como o CERT.br, aberto a todo o público brasileiro e vinculado ao CGI.br, o CTIR-GOV, que serve a Administração Pública Federal, e outros específicos como o GRIS-Correios, CSIRT CAIXA, CSIRT UOL e CSIRT Unicamp.

O estudo e a prática da segurança cibernética pelo Estado brasileiro remonta à criação do Gabinete de Segurança Institucional (GSI/PR) pela Presidência da República, através do Decreto no 3.505/2000. Órgãos associados ao gabinete tratar de questões específicas da "defesa cibernética" foram criados nos anos subsequentes. *[BRASIL-CIBERSEG-2015]* (Página 109)

Um dos principais catalisadores da infraestrutura de defesa cibernética brasileira foi a CPI da Espionagem, "destinada a investigar a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos Estados Unidos, com o objetivo de monitorar e-mails, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas ou protegidas pela Constituição Federal".

Uma das recomendações da Comissão Parlamentar de Inquérito que foram levadas à cabo pelo governo federal foi a elaboração de uma Estratégia Nacional de Segurança Cibernética, em que "sejam delineadas as principais medidas de segurança cibernética para o Estado brasileiro,

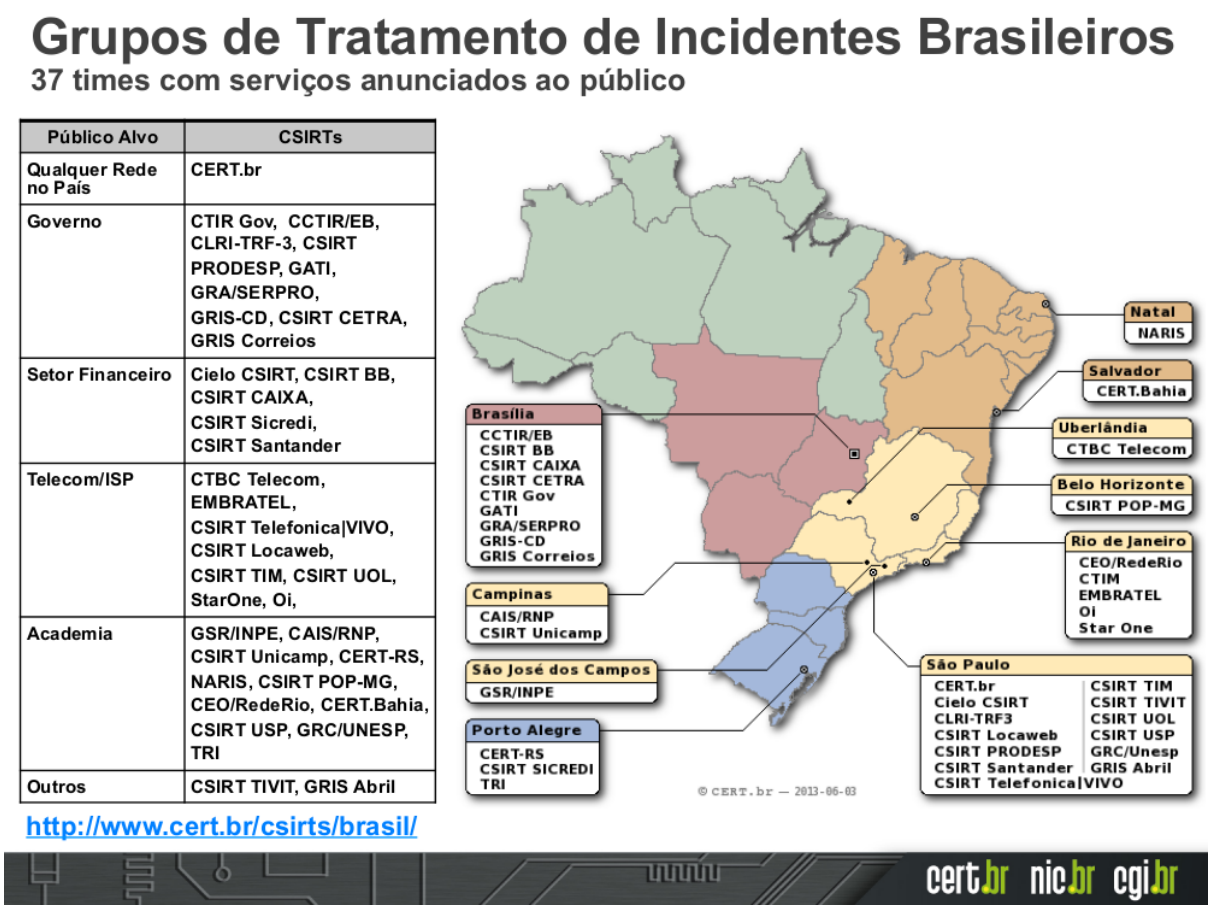


Fig. 10.1: Mapa dos grupos de tratamento de incidentes de segurança brasileiros, feito em junho de 2013 e apresentado por Cristine Hoepers, gerente geral do CERT.br/NIC.br, em setembro de 2015.

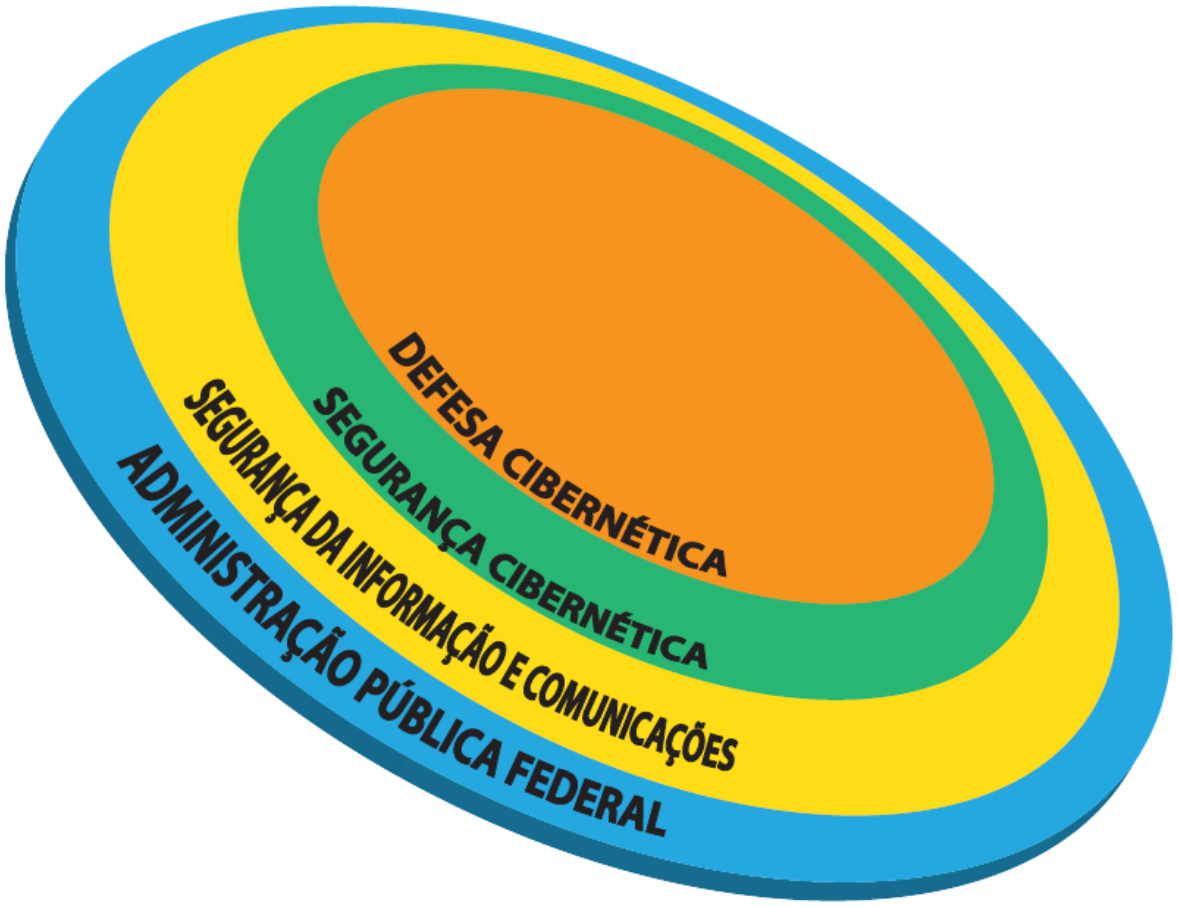


Fig. 10.2: Visão em camada da estratégia brasileira de segurança da informação e comunicação, de segurança e defesa cibernética. *[BRASIL-CIBERSEG-2015]* (Página 109)

englobando ações coordenadas entre os setores público e privado".

No documento resultante, escrito pelo Departamento de Segurança da Informação e Comunicações (DSIC) e sugestivamente nomeado "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal", conta-se a história da segurança da informação e cibernética na estratégia de defesa do país através de "marcos do governo brasileiro em SIC e SegCiber".

Após a criação do GSI/PR, foram estabelecidas ao longo dos anos diversas parcerias com setores específicos do governo, como a Controladoria Geral da União, o Banco do Brasil e a Caixa Federal, a Petrobrás, o INSS e a SERPRO, "com a finalidade de organizarem atividades em conjunto que possibilitassem a disseminação da cultura da Segurança da Informação". Também são registrados os acordos de "Troca e Proteção Mútua de Informações Classificadas" que o Brasil assinou com Portugal, Espanha, Rússia, Itália, Israel e Suécia.

Na seção "Contextualização", os(as) autores(as) contam com mais detalhes o crescimento dos órgãos de apoio ao GSI/PR:

> No Brasil, os assuntos relacionados à Segurança da Informação e Comunicações, Segurança Cibernética e Segurança das Infraestruturas Críticas vêm sendo tratados no âmbito do **Conselho de Defesa Nacional (CDN)** e da **Câmara de Relações Exteriores e Defesa Nacional (CREDEN)**, do Conselho de Governo, por intermédio do **Gabinete de Segurança Institucional da Presidência da República (GSI/PR)**, que exerce as funções de Secretaria Executiva do citado Conselho e de Presidência daquela Câmara.
>
> [...]
>
> A dimensão e a assimetria da APF representa importante desafio para a área de SIC e de SegCiber. Na atualidade, são 39 ministérios, cerca de seis mil entidades governamentais, mais de um milhão de servidores federais, em torno de 320 grandes redes do Governo Federal, mais de 16,5 mil sítios de governo que superam 12 milhões de páginas WEB, e uma crescente participação e controle social.
>
> O GSI/PR, diante de tal desafio, instituiu em 2006, para trato das questões afetas à SIC e à SegCiber, **o Departamento de Segurança da Informação e Comunicações (DSIC), com abrangência de atuação na APF**, e três áreas finalísticas para o cumprimento de sua missão, a saber: **Gestão de SIC**, **Centro de Tratamento de Incidentes de Redes da Administração Pública Federal - CTIR Gov**, e **Credenciamento de Segurança**.
>
> [...]
>
> A **Agência Brasileira de Inteligência (ABIN)**, órgão vinculado ao GSI/PR, conta em sua estrutura com o **Centro de Pesquisas e Desenvolvimento para Segurança das Comunicações (CEPESC)**, criado em 1982 para sanar deficiência do Brasil em garantir o sigilo dos canais de comunicação dos órgãos estratégicos da Administração Pública Federal. Desde então, vem desenvolvendo **soluções de segurança da informação e comunicações** baseadas em algoritmos criptográficos de Estado, bem como executando **trabalhos de pesquisa e desenvolvimento** na área da segurança cibernética.
>
> Assim, na última década, os **temas de SIC e de SegCiber passaram a ser** reco-

nhecidos por vários atores do Governo Federal como relevantes e **de competência e coordenação político estratégica de órgão da Presidência da República**, com abrangência para a APF, incluídas ações de segurança das infraestruturas críticas da informação. *[BRASIL-CIBERSEG-2015]* (Página 109)

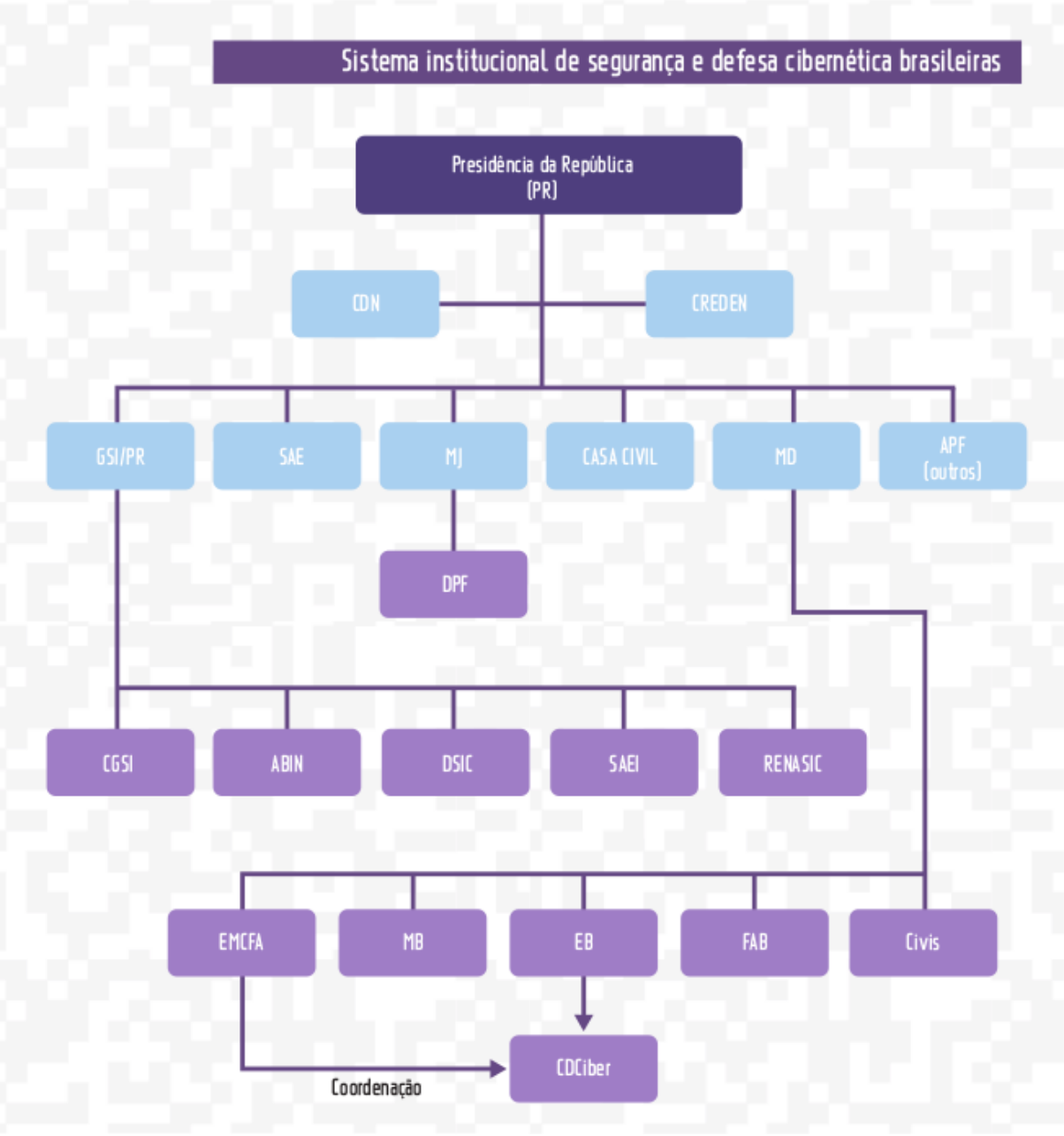


Fig. 10.3: Organograma do sistema institucional de segurança e defesa cibernética brasileiras. *[BRASIL-CIBERSEG-2015]* (Página 109)

A história e a organização institucional da segurança e da defesa cibernética no Brasil é muito bem contada em Da Cibersegurança à Ciberguerra *[ARTIGO19-CIBERSEG-2016]* (Página 108), uma análise crítica da ONG ARTIGO 19 sobre o uso potencial de equipamentos e softwares de vigilantismo ou ofensivos como parte da estratégia nacional de defesa cibernética.

Fig. 10.4: Relatório Da Cibersegurança à Ciberguerra, da ARTIGO 19.

10.3 Cenário internacional

Algumas organizações internacionais se destacam tanto por sua abordagem no âmbito da segurança cibernética e da informação quanto pela participação do Brasil em seus processos de deliberação e decisão multissetorial (onde são ouvidos tanto representantes de governos quanto de empresas, da sociedade civil, academia e outros setores da sociedade) .

10.3.1 Organização dos Estados Americanos (OEA / OAS)

Segundo conta Carolina Rossini, vice-presidente e coordenadora de política internacional da organização de acesso à informação Public Knowledge, o fortalecimento da segurança cibernética de seus países-membro é uma das prioridades da OEA:

> Em resposta ao aumento das ameaças cibernéticas identificadas, a Organização dos Estados Americanos (OEA), através do Comitê Interamericano Contra o Terrorismo (CICTE), vem desenvolvendo um programa regional de segurança cibernética que busca fortalecer a segurança e melhorar a proteção da infraestrutura de informação crítica em todo o continente.
>
> Assim, desde o começo da década da passada, a OEA investe na segurança cibernética por meio de uma série de atividades em parceria com especialistas, empresas e governos da região. Em 2004, a OEA publicou a "Declaração sobre o Fortalecimento da Segurança Cibernética nas Américas", pedra fundamental para o desenvolvimento e a publicação do relatório "Estratégia Interamericana Integral para Combater as Ameaças à Segurança Cibernética", em 2012.

> A declaração de 2004 significou o reconhecimento por parte dos Estados Membros da OEA de que combater os crimes cibernéticos e fortalecer a resiliência cibernética eram questões imperativas para o desenvolvimento econômico e social, a governança democrática, a segurança nacional e dos cidadãos. *[ROSSINI-OEA-2015]* (Página 113)

Além de publicar relatórios sobre a situação da segurança cibernética no continente americano e guias de boas práticas, a OEA também articula atividades e eventos em parceira com organizações de segurança para promover a cultura de segurança e melhorar estruturas de resposta a incidentes.

O governo brasileiro, através do Gabinete de Segurança Institucional, dialoga com a OEA na área digital, participando inclusive de eventos estratégicos, como é relatado no Livro Verde: Segurança Cibernética no Brasil:

> Uma iniciativa que vale frisar é a adoção, pela OEA, desde 2004, de uma "Estratégia Interamericana Integral para Combater as Ameaças à Segurança Cibernética", visando a criação de uma cultura de segurança cibernética para lutar contra as ameaças aos cidadãos, à economia e aos serviços essenciais, que não possam ser enfrentadas por um único governo ou combatidas por meio de uma disciplina ou prática solitária. No ano de 2009, o "Workshop Hemisférico Conjunto da OEA sobre o Desenvolvimento de uma Estrutura Nacional para Segurança Cibernética" foi realizado de 16 a 20/Nov/2009, contando na organização, além do Governo brasileiro, anfitrião, por intermédio do GSIPR, da OEA representada pelos seguintes fóruns: Comitê Interamericano contra o Terrorismo Cibernético (CICTE), Comissão Interamericana de Telecomunicações (CITEL), e, Reunião de Ministros da Justiça ou Procuradores Gerais das Américas (REMJA), o que fortaleceu o papel do Brasil como um dos protagonistas no tema;

Um dos últimos relatórios sobre segurança cibernética publicados pela OEA em parceria com o Banco Interamericano de Desenvolvimento (BID / IDB) é o "Cybersecurity: Are We Ready in Latin America and the Caribbean?". Em um prefácio, o secretário geral da OEA, Luis Almagro, conta sobre o programa de segurança cibernética da OEA se origina de seu comitê antiterrorismo (tradução nossa):

> O Programa de Segurança Cibernética [Cybersecurity Program] da Comitê Interamericano contra o Terrorismo (CICTE).teve um papel chave nesta frente. O programa ajudou os Estados Membros a desenvolver Estratégias Nacionais de Segurança Cibernética, providenciou treinamento para a Equipes de Resposta a Incidentes de Segurança de Computadores [Computer Security Incident Response Teams] (CSIRT), facilitou exercícios de gestão de crise com operadores da indústria nacional crítica e setores de resposta de emergência, se engajou com a sociedade civil e o setor privado, e ajudou a trazer visibilidade à ameaças relacionadas à segurança da informação e oportunidades dentro da nossa região. Dessas e outras maneiras, o CICTE tem diretamente contribuído para um domínio cibernético mais seguro e vigilante no Caribe e na América Latina. *[OEAeBID-CIBERSEGLATAM-2016]* (Página 112)

A Public Knowledge, no módulo Ciberseguridad y Derechos Humanos de seu curso Internet Libre y Abierto da P2PU, analisa a atuação da OEA na seção "segurança cibernética e relações internacionais" (tradução nossa):

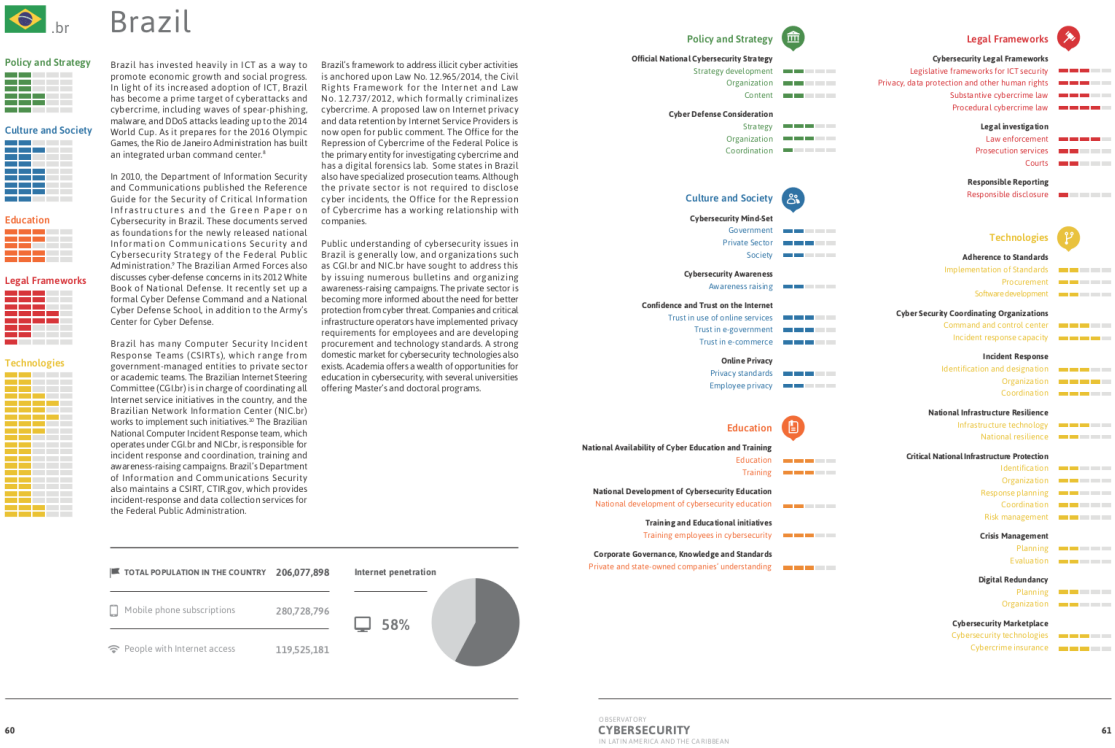


Fig. 10.5: Perfil da segurança cibernética do Brasil em ampla análise da América latina e do Caribe feita pela OEA e o BID, a partir de contribuições do governo (ABIN, DSIC, CTIR-GOV, GSI/PR) e da sociedade civil (CTS/FGV, CGI.br, ITSRio) *[OEAeBID-CIBERSEGLATAM-2016]* (Página 112) (páginas 60 e 61).

> Em 2004, os Estados Membros da OEA adotaram de forna unânime a Estratégia Interamericana Integral para Combater as Ameaças à Segurança Cibernética; como a maioria das estratégias sobre segurança cibernética, ela tem o foco principal no crime e on terrorismo cibernético, deixando de lado outros aspectos da segurança cibernética. O espírito da resolução revela uma tendência progressiva na América Latina para a aplicação não só da doutrina da justiça penal e da segurança pública, mas também da doutrina militar, nas estratégias de segurança cibernética, e assim destaca a *Análise de referência de processos e eventos relativos às TIC: Implicências para a segurança internacional e regional <http://ict4peace.org/baseline-review-of-ict-related-processes-and-events-implications-for-international-and-regional-security/#sthash.8X8nxU44.dpuf>*.

A OEA vem dialogando com a sociedade civil em seus relatórios, eventos e treinamentos. No relatório Cybersecurity citado acima, há uma *expert contribution* escrita por pesquisadores(as) do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas (CTS/FGV): Cybersecurity, Privacy and Trust: Trends in Latin America and the Caribbean ("Segurança Cibernética, Privacidade e Confiança: Tendências na América Latina e no Caribe").

Na contribuição, Marília Maciel, Nathalia Foditsch, Luca Belli e Nicolas Castellon aponta algumas características do campo na região: conscientização da importância de estratégias de segurança cibernética; o exército e agências de segurança nacional não foram amplamente estabelecidas como coordenadores das políticas; há alguma colaboração multissetorial notável pela presença e colaboração entre CSIRT's (equipes de resposta a incidentes) na região; muitos países vêm criando um alterando leis de forma precipitada para o combate ao crime cibernético; há um aumento substancial na preocupação com a privacidade e a proteção dos dados pessoais – que, segundo o documento, é incompatível com a retenção de dados em massa [OEAeBID-CIBERSEGLATAM-2016].

Para o caminho à frente no campo da segurança cibernética, o grupo recomenda (tradução nossa):

- Definir e fazer valer marcos regulatórios coerentes de privacidade e proteção de dados: "é essencial balancear a provisão de segurança com a necessidade de proteger aprorpiadamente os direitos dos indivíduos. [...] Também é necessário balancear os custos e benefícios da existência de provisões de retenção de dados."
- Criar plataformas nacionais multissetorial sustentáveis: "grupos da sociedade civil, as comunidades acadêmicas e técnicas, e representantes da indústria são capazes de prover *expertise* valiosos através de suas perspectivas, e ajudar a criar marcos regulatórios coerentes de uma maneira sustentável."
- Fortalecer a cooperação internacional: "é importante criar canais para cooperação em vários níveis entre governos nacionais e organizações regionais ou globais trabalhando na área. [...] a natureza da Internet de não ter fronteiras aumenta a importância da cooperação internacional e da harmonização de dispositivos legais."

10.3.2 Organização para Cooperação e Desenvolvimento Econômico (OECD / OCDE)

A OECD, fundada em 1961 para estimular o progresso econômico e o comércio global. Entre diversos tópicos como educação, ciência e tecnologia, agricultura e relações públicas, a organização também aborda a segurança digital.

Através de um processo multissetorial iniciado em 2012 pelo Working Party on Security and Privacy in the Digital Economy ("grupo de trabalho em segurança e privacidade na economia digital"), a OECD publicou o documento Recommendation on Digital Security Risk Management ("recomendações sobre gestão de riscos de segurança"), onde delineia os caminhos que os Estados devem trilhar para proteger suas infraestruturas e processos críticos de ataques digitais em harmonia com direitos fundamentais, em torno de 8 princípios (traduções nossas):

- Percepção, habilidades e empoderamento (*awareness, skills and empowerment*)
- Responsabilidade e prestação de contas (*responsibility*)
- Direitos humanos e valores fundamentais (*human rights and fundamental values*)
- Cooperação (*co-operation*)
- Reconhecimento de riscos e ciclos de tratamento (*risk assessment and treatment cycle*)
- Medidas de segurança (*security measures*)
- Inovação (*innovation*)
- Prestatividade e continuidade (*preparedness and continuity*) *[OECD-RISK-2015]* (Página 112)

A OECD prefere tratar o tema através do conceito de *riscos de segurança digital*, em vez da segurança cibernética, por sua maior clareza e por trazer a segurança de um tema meramente técnico para o econômico e social (tradução nossa):

> Em vez de ser tratado como um problema técnico que pede soluções técnicas, o risco digital deve ser abordado como um risco econômico; ele deve então ser uma parte integral dos processos gerais de gestão de risco e tomada de decisão de uma organização. A noção de que riscos de segurança digital merecem uma resposta fundamentalmente diferente em sua natureza das outras categorias de riscos precisa ser combatida. Para este efeito, o termo "segurança cibernética e de forma mais geral o prefixo "ciber" que ajudaram a transmitir este senso errôneo de especificidade não aparecem nas Recomendações de 2015.

Embora as recomendações não tenham efeito legal vinculante ("*non-legally binding*"), o peso da OECD como organização é claro. Os atos da organizção "na prática possuem grande força moral, pois representam a vontade política dos países membros", segundo o documento anexo às Recomendações:

> É importante destacar que as Recomendações, e de modo mais geral o trabalho da OECD na área [de segurança digital], é parte de um diálogo internacional envolvendo várias organizações, com fluxos complementares de trabalho refletindo seus mandatos. Por exemplo, o Conselho da Europa endereçou questões relacionadas ao crime cibernético (por exemplo, na Convenção de Budapeste sobre o Crime

> Cibernético); a Interpol facilita a cooperação operacional entre agentes da lei; as Nações Unidas e a Organização para Segurança e Cooperação na Europa (OSCE) discute o comportamento dos Estados no meio digital e medidas de construção de confiança para preservar a estabilidade nacional; padrões técnicos estão sendo desenvolvidos em uma variedade de ambientes como a International Organization for Standardization (ISO), a Internet Engineering Task force (IETF), a World Wide Web Consortium (W3C), a Organization for the Advancement of Structured Information Standards (OASIS), etc. Organizações regionais como a Asia-Pacific Economic Cooperation (APEC) também desepenham um papel-chave para estimular a implementação das melhores práticas e orientações. *[OECD-RISK-2015]* (Página 112)

Embora o Brasil não seja um país membro da OECD, em 2007 seu Conselho Ministerial estabeleceu um acordo de "engajamento aprimorado", como um esforço originado em 2003 pelo Embaixador do Japão para a OECD Seiichiro Noboru para alargar a cooperação com países não-membros. Além do Brasil, também firmaram o acordo a China, Índia, Indonésia e África do Sul, selecionadas através de quatro critérios: "afinidade de pensamento" (*like-mindedness*), "ator relevante" (*significant player*), "benefício mútuo" (*mutual benefit*) e "considerações globais" (*global considerations*). *[OECD-ENGAGEMENT-2015]* (Página 112).

O Brasil assinou em 2014 um "tratado multilateral de autoridade competente" estabelecido em reuniões da OECD para combater a sonegação de impostos. O tratado prevê o compartilhamento de dados financeiros sobre impostos com os outros países participantes; o Brasil começará a incluir os seus a partir de 2018.

Mas talvez seja no campo da segurança cibernética que se dá a maior participação do Brasil na OECD.

Já em 2010, na publicação do Livro Verde: Segurança Cibernética no Brasil pelo GSI/PR, as recomendações da OECD (na prática, uma versão anterior da supracitada *[OECD-RISK-2015]* (Página 112)) eram citadas como ponto de partida para compreender as "competências essenciais da segurança cibernética".

No mesmo documento, a participação do Brasil em um evento da OECD é citado como evidência do Brasil sendo "um dos protagonistas em iniciativas e fóruns internacionais" e de sua "competência articuladora, de gestão e técnica" no tema:

> A participação de representante do Brasil, do GSIPR, na categoria de observador ad hoc no "Working Party on Information Security and Privacy - WPISP", e do "Comittee for Information, Computer and Communications - ICCP", promovidos pela "Organização para Cooperação e Desenvolvimento Econômico - OCDE", realizados em Paris/França, em 2009 e 2010, também merece destaque. Por ocasião da reunião de 2010, o Brasil apresentou proposta de realização de "Estudo comparativo das estratégias nacionais de segurança cibernética"; a qual foi plenamente aceita e, para tanto, foi criado Grupo com presença de países voluntários para tal finalidade. O Grupo é presidido pelo representante de Portugal na OCDE, e conta com a participação dos seguintes países: Portugal, EUA, Coréia, Austrália, Japão, Espanha, e Brasil. *[BRASIL-VERDE-2010]* (Página 109)

A sociedade civil brasileira também tem se aproximado da OECD no que tange políticas de segurança cibernética e gestão de riscos de segurança digital. Na organização, o diálogo com a

sociedade civil se dá através do CSISAC, Civil Society Information Society Advisory Council, criado a partir de uma declaração feita na Conferência Ministerial sobre o Futuro da Economia da Internet, ocorrida em Seoul, Coréia do Sul, em junho de 2008.

Além do pedido de criação de um conselho da sociedade civil, a Declaração de Seoul também chama a atenção dos(as) Ministros(as) para diversos temas, trazendo recomendações específicas para cada um (tradução nossa):

- Liberdade de expressão
- Proteção da privacidade e transparência
- Proteção do(a) consumidor(a)
- Emprego, trabalho digno e habilidades
- Promoção do acesso ao conhecimento
- Governança da Internet
- Promoção de padrões abertos e neutralidade da rede
- Políticas de direitos autorais balanceadas
- Apoio a mídias pluralísticas
- Sociedade digital inclusiva
- Diversidade cultural *[OECD-SEOUL-2008]* (Página 112)

Em junho deste ano, a OECD realizará seu encontro Ministerial anual, reunindo os ministros da economia de todos os países membro. Com o foco principal na Economia Digital, o Ministerial será dividido em quatro tópicos, sendo um deles a Confiança na Economia Digital, com um painel intitulado Gerindo o Risco Digital (a OECD prefere esse termo à "segurança cibernética", como já explicado). O Brasil será representado, através do CSISAC, por organizações sem fins lucrativos como a ARTIGO 19, Coding Rights, InternetLab, Instituto Beta para Internet e a Democracia e CTS/FGV, que constam como Grupos de Referência do CSISAC Forum, um encontro realizado junto com o Ministerial que reunirá a sociedade civil organizada para deliberar a atuação do CSISAC no evento principal.

10.3.3 International Telecommunication Union (ITU / UIT)

A União Internacional das Telecomunicações, sediada em Genebra, Suíça, possui a missão de orientar o crescimento e desenvolvimento sustentável das telecomunicações e redes de informação, e possui 192 Estados-membros, incluindo o Brasil.

Como vimos, a organização conduziu um estudo sobre segurança cibernética entre 2005 e 2008, materializado em sua Recommendation ITU-T X.1205, "Visão geral da segurança cibernética", onde definem o conceito e analisam estratégias de proteção e técnicas de ataque. *[ITU-CIBERSEG-2008]* (Página 115)

A UIT também aborda o campo através de sua Global Cybersecurity Agenda (tradução nossa):

Lançada em 2007 pelo então Secretário-Geral da UIT, Dr. Hamadoun I. Touré (2007 - 2014), a ITU Global Cybersecurity Agenda (GCA) é um sistema para cooperação internacional destinado a aumentar a confiança e a segurança na sociedade da informação. A GCA foi projetada para a cooperação e a eficiência, encorajando a colaboração com e entre todos os parceiros relevantes e com base em iniciativas existentes para evitar a duplicação de esforços. *[ITU-GCA]* (Página 115)

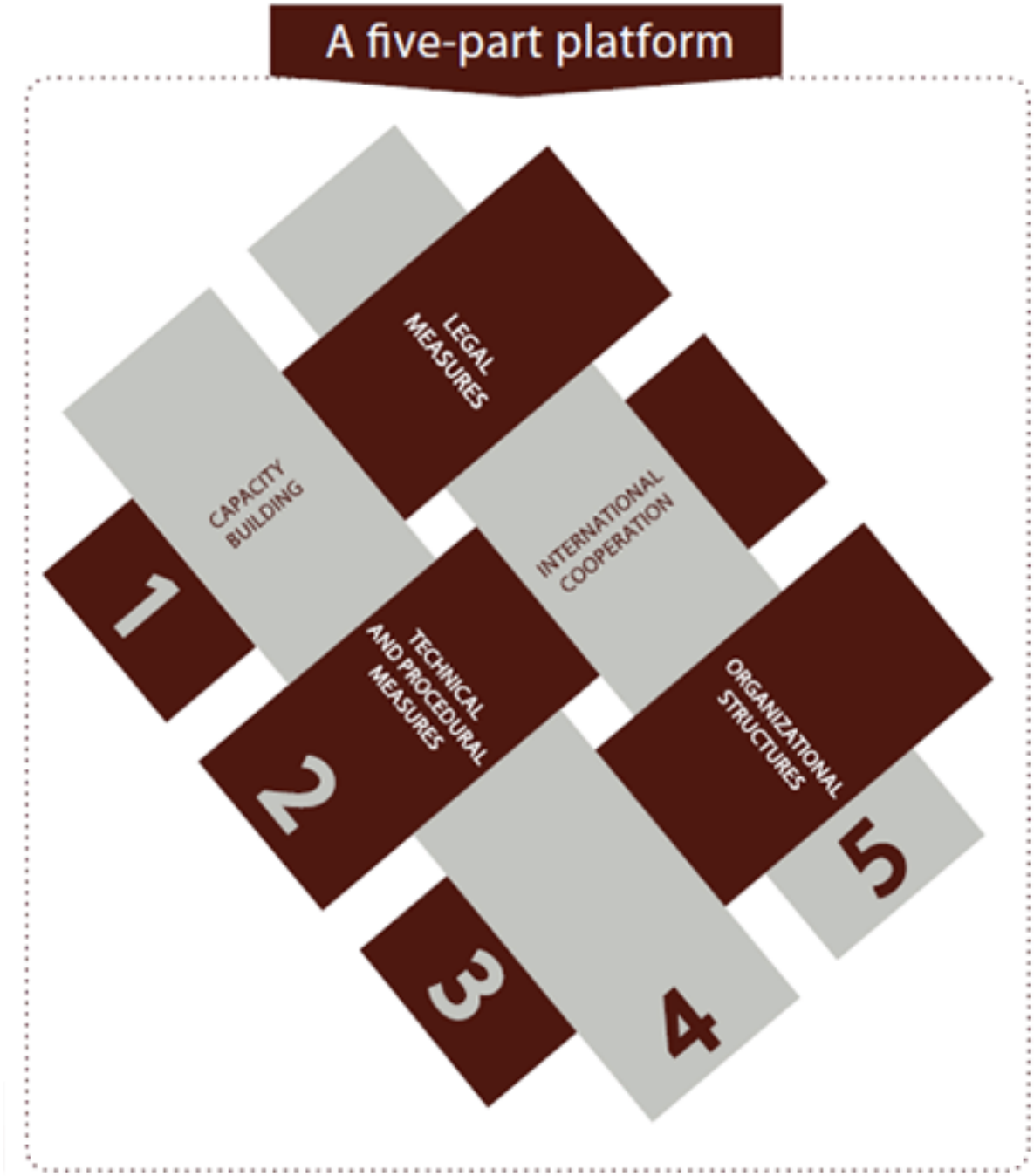


Fig. 10.6: Ilustração dos cinco pilares estratégicos, ou áreas de trabalho (*work areas*) da Global Cybersecurity Agenda: medidas legais, medidas técnicas e procedurais, estruturas organizacionais, capacitação e cooperação internacional.

CAPÍTULO 11

Questões Emergentes

11.1 Deep Web

A *deep web*, um conceito que é muito confundido e virou sinônimo da *rede onion* (ver subseção abaixo), não é de relevância particular no contexto desta CPI – seus sites operam sob as mesmas regras e restrições dos que se pode encontrar em buscadores como o Google. Como a apropriação já está em uso (na própria comissão e no vocabulário popular, cabe reforçar este fato: **a deep web joga sob as mesmas regras técnicas e jurídicas que os outros sites da web**.

A deep web compreende todas as páginas web (ou seja, tudo que pode ser acessado pelo navegador) que não estão indexadas e catalogadas nos grandes mecanismos de busca, como Google, Bing e DuckDuckGo. O termo foi inicialmente cunhado para representar a grande parcela da web que não pode ser encontrada nestes portais, indicando que a web é muito maior do que parece à primeira vista – daí a metáfora comum da web "superficial" como a ponta de um iceberg.

Já o termo *dark web* significa a rede de sites acessíveis através de softwares específicos (geralmente o Tor) que *não revelam seu local geográfico* para quem as acessam, *não podem ser bloqueados* e cuja interação com seus usuários é *tecnicamente inviolável*.

Como estas características impedem alguns procedimentos comuns de policiais e juízes, ela por diversas vezes foi trazida à CPI como um problema a ser combatido ou criminalizado, mas nós acreditamos que os obstáculos investigativos devem ser avaliados em contraste com seu amplo uso como ferramenta para a garantia da liberdade de expressão, como na proteção contra monitoramento *online* abusivo, espionagem industrial ou internacional, no combate à corrupção e recebimento de denúncias anônimas, na instrumentalização do sigilo da fonte jornalística, entre outros fins protegidos pela nossa própria Constituição, por tratados e organizações internacionais.

Justamente por causar confusão quanto ao seu objetivo por lembrar "escuridão", o termo "dark web" está em desuso; e o nome dado pelo Projeto Tor, pela comunidade que promove e trabalha no projeto e pela mídia especializada é **onion web**. Assim como a web "tradicional" é uma parte da Internet, a *onion web* é parte da *rede onion*.

Veja também:

Anonimato Online (Página 37)

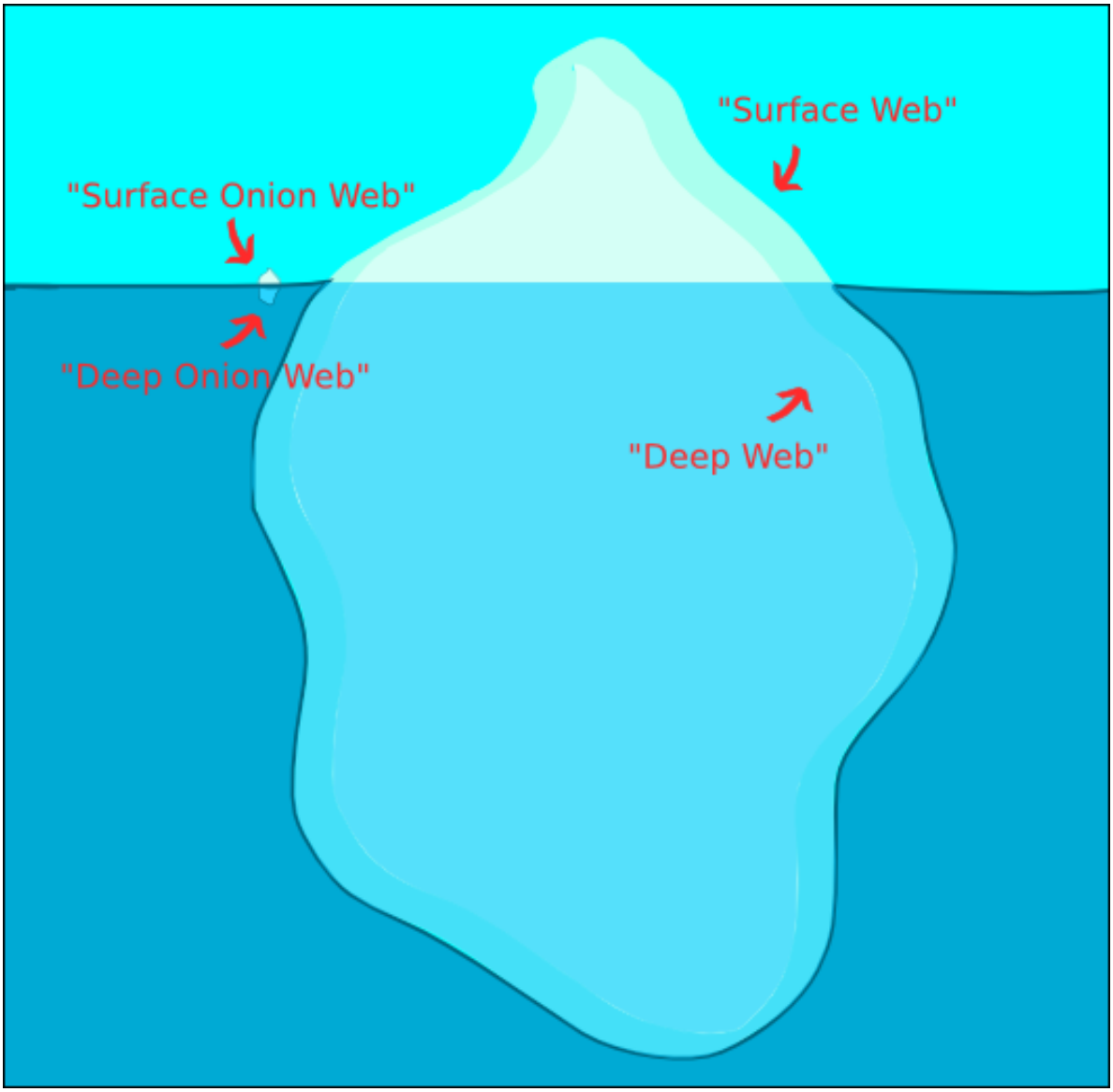
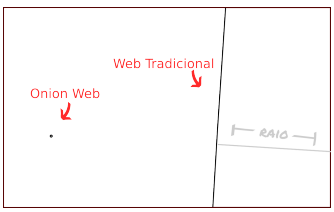


Fig. 11.1: Esta representação transforma a representação usual da deep web, com a web superficial na ponta, em contraste com a *onion web*, que dentro da mesma metáfora deve ser representada como um iceberg à parte, com sua própria "*onion web* superficial", indexada em sites como o Ahmia, e a sua "*deep onion web*". A proporção entre os icebergs é ilustrativa; numa escala real, o iceberg *onion* ficaria menor que um pixel (todas as estimativas apontam para menos de 50 mil sites *onion*, versus os 900 milhões de sites na web aberta contabilizados em dezembro de 2015 pela Netcraft).



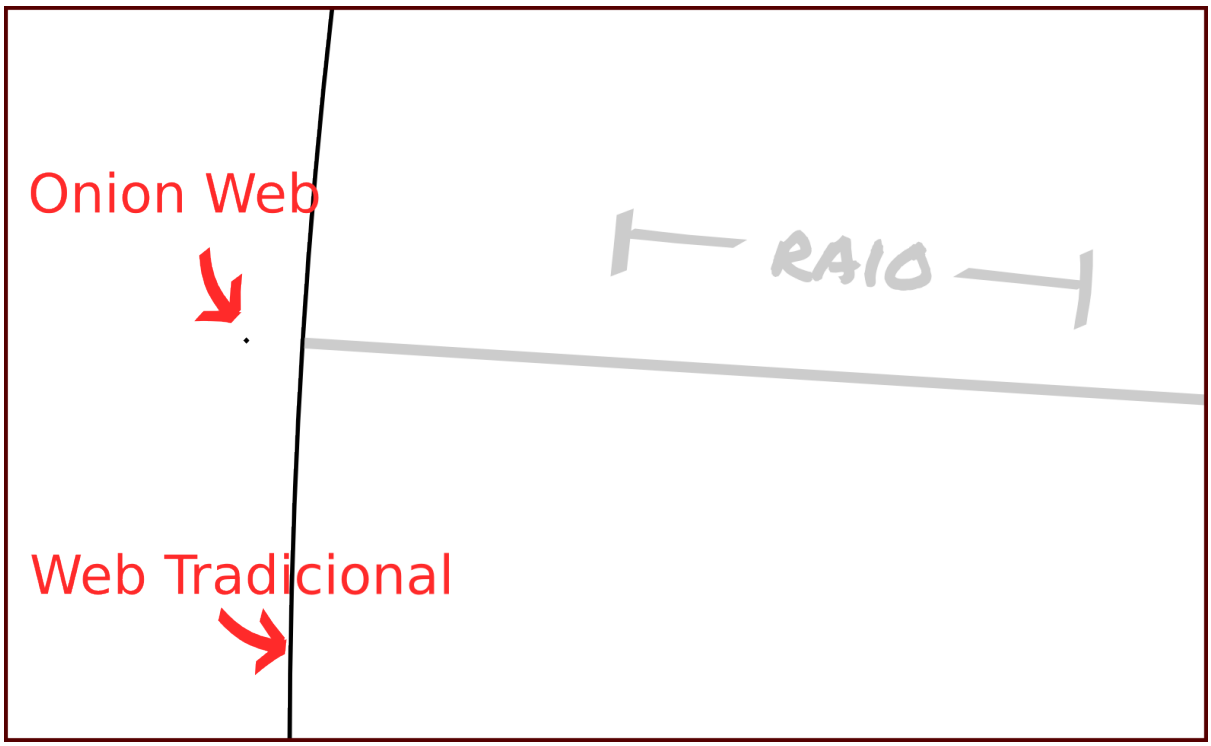


Fig. 11.2: Representação da "onion web" e da web tradicional, na real proporção de acordo com os mesmos números (50 mil websites onion, um teto generoso, versus 900 milhões de sites na web de acordo com a Netcraft – 18.000x mais)

É possível...	Web "superficial"	Web + Tor	Deep Web	Onion Web	Deep Onion Web
Buscar sites nos serviços tradicionais	**Sim**	**Sim**	*Não*	*Não*	*Não*
Buscar com sistemas especializados	**Sim**	**Sim**	De-pende*	**Sim**	Depende*
Localizar usuário(a)	**Sim**	*Não*	**Sim**	*Não*	*Não*
Localizar servidor	**Sim**	**Sim**	**Sim**	*Não*	*Não*

* Páginas que os buscadores tradicionais meramente não se deram o trabalho de processar e indexar sim; páginas que precisam de *login* para serem acessadas, não.

11.2 Pornografia Infantil

Uma das preocupações específicas manifestada nesta CPI sobre a rede *onion* é o seu uso para envio de pornografia infantil.

Em recente conversa organizada pelo Instituto Educadigital com o tema "por uma internet mais positiva", o diretor de educação da Safernet Rodrigo Nejm disse que o Brasil "não é um produtor de pornografia infantil":

> A gente [da Safernet] sempre disse isso mas agora a gente vê que até mesmo na imprensa isso está mais claro, e mais fraco este discurso de que no Brasil o maior

> problema é a pornografia infantil na Internet [...] é muito bom que a gente possa ampliar a pauta e passar pra uma discussão mais além do pânico moral.

A Safernet, que já foi representada na CPICIBER por Thiago Tavares, presidente da organização, trabalha no combate à pornografia infantil e vários outros crimes, através de redes internacionais como a INHOPE, a InSafe e a Child Helpline International.

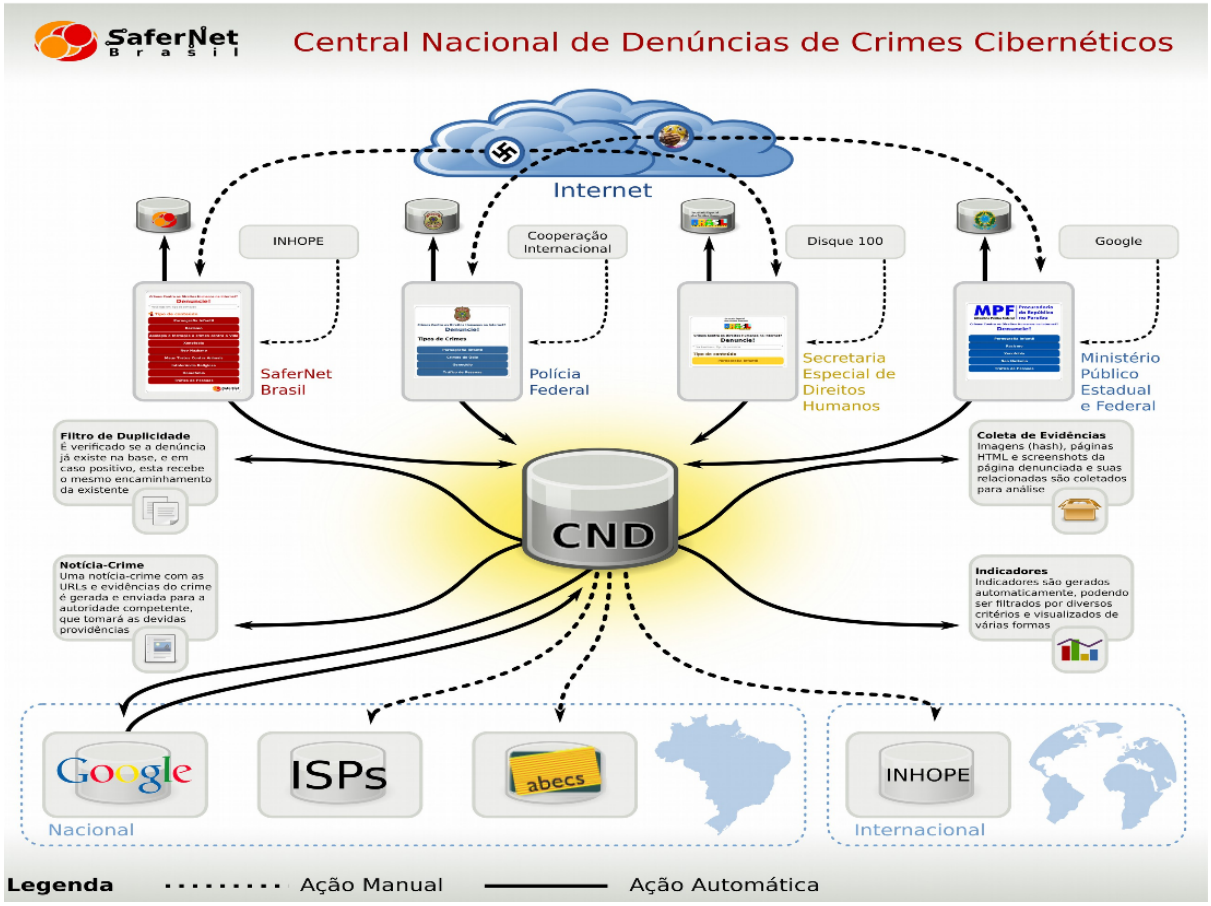


Fig. 11.3: Organograma do funcionamento da Central Nacional de Denúncias de Crimes Cibernéticos, que coordena a Safernet com a Secretaria Especial de Direitos Humanos, a PF e o MPF, provedores de conexão e aplicação, e organizações de cooperação internacional. Apresentado por Thiago Tavares na CPICIBER.

Além de receber e encaminhar denúncias, o trabalho da Safernet é também muito focado na educação de crianças, adolescentes e o público em geral no uso da Internet para que os abusos e crimes nem cheguem a acontecer – e ferramentas de anonimato são parte dos temas abordados. Conforme conta Rodrigo Nejm:

> [A SaferNet produziu] um guia chamado "Internet Que Queremos", que é feito para adolescentes discutirem rastros digitais, privacidade, liberdade de expressão, anonimato, saber a importância do anonimato, diferenciar ele de outras situações e assim por diante. [...] A ideia é de uma vez por todas superar o pânico moral e investir pesado nessa educação para a cidadania digital.

Em um painel do re:publica 2015 sobre a rede *onion*, o oficial de polícia alemão Heiko Rittelmeier perguntou ao pesquisador de segurança e membro do Projeto Tor Jacob Appelbaum

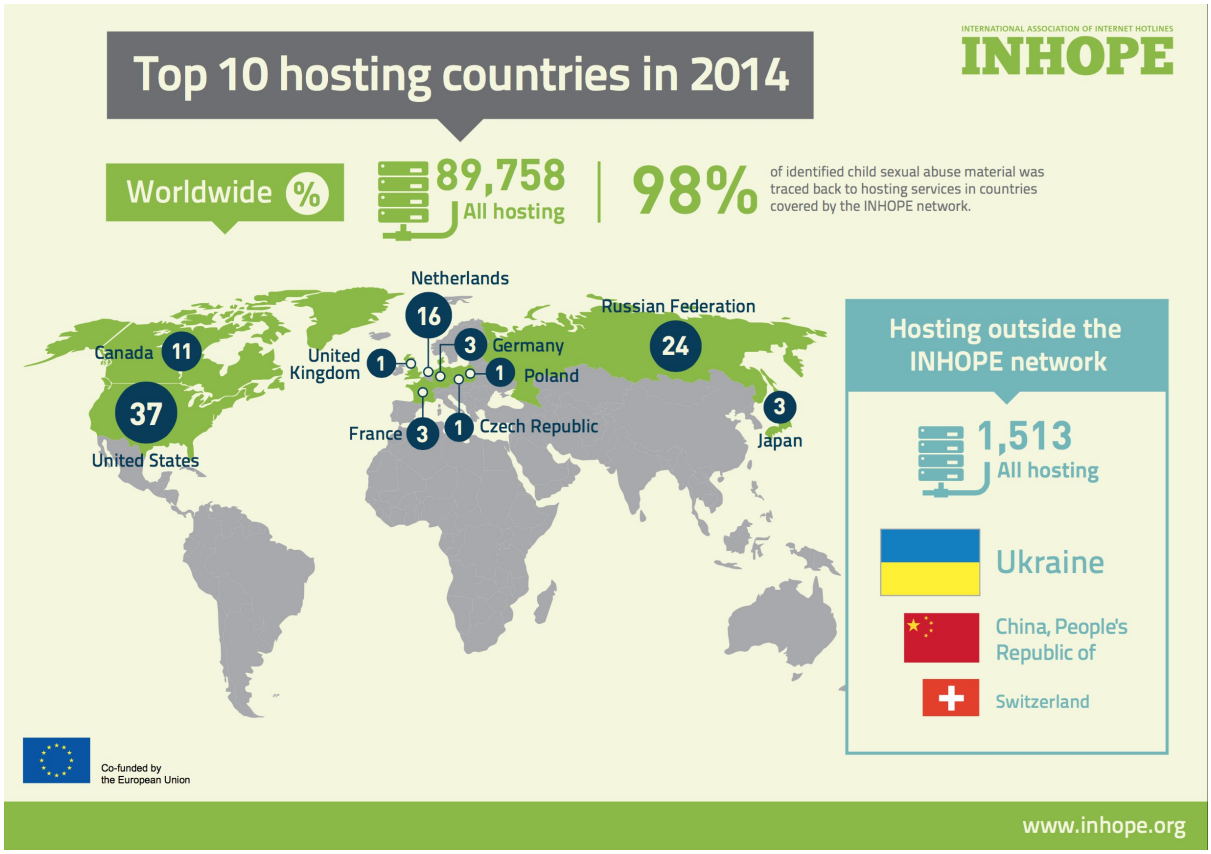


Fig. 11.4: Infográfico da INHOPE mostrando a localização dos principais provedores de pornografia infantil. Apresentado por Thiago Tavares na CPICIBER.

sobre a possibilidade de banir sites de pornografia infantil da rede. Jacob explicou como, além de inevitavelmente *ferir a liberdade de conexão* (Página 57) e pôr vários outros conteúdos em risco, combater desesperadamente os sintomas não ajudará a tratar as causas da doença:

> O problema com a pornografia infantil não é que se pode vê-la e que agora há evidência dela. O fato de que alguém pode ver que há uma epidemia de pessoas causando danos a crianças é obviamente um problema. Mas não se pode ignorar que tal epidemia existe. E é melhor que a polícia tenha acesso a isso para que tenha evidências e possa de fato seguir o rastro dessas pessoas e ir até a raiz do problema.
>
> E qual é a raiz do problema? Não é o anonimato. O problema é que pessoas estão esuprando e abusando de crianças. Da mesma maneira que a câmera polaroid não era o problema, o Tor também não é. Esta é problema sistêmico da sociedade, e para resolvê-lo é necessária cooperação internacional. [...] Se você esconde [o problema], você não resolve a causa sistêmica. Se você o expõe, então sabe que precisa procurar pelas raízes sistêmicas e lutar contra elas radicalmente. Talvez você tenha que tomar ações drásticas, e talvez alguns criminosos, algumas vezes, escapem. Mas com certeza será impossível ignorar o cerne, o problema verdadeiro.
>
> Muitas pessoas dirão que "é um problema que se possa ver este tipo de coisa", ou que "é um problema que isto esteja sendo compartilhado". E *é*, mas é um problema menor se comparado ao das pessoas que estão fazendo mal a crianças de verdade; então lhe pergunto: "*você não pensa nas crianças?*"
>
> Nós geralmente ouvimos isso na direção oposta: "vamos nos livrar do anonimato porque... pensem nas crianças!", mas se você remover o anonimato, você não vai estar ajudando as crianças de verdade, e de fato retirando delas uma das únicas ferramentas disponíveis gratuitamente para as crianças se protegerem na Internet.
>
> [...] Temos que enfrentar o cerne do problema; o abuso de crianças é um problema social, e não vamos resolvê-lo tecnologicamente, mas socialmente, e temos que fazer isto em escala global. Isso significa que temos que respeitar os direitos das crianças, e parte destes direitos, [no caso de comprometer o Tor], estão muito claramente sendo violados. Então vamos trabalhar em encontrá-los mas não comprometendo o sitema de anonimato.

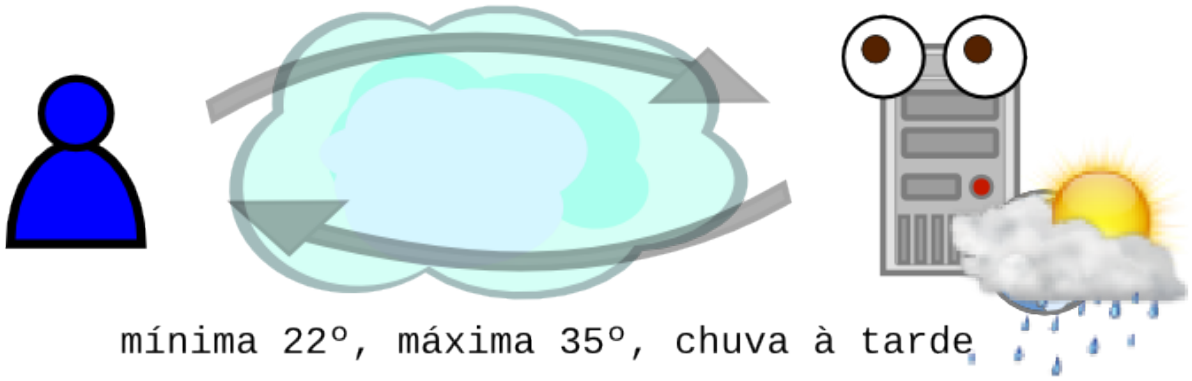
11.3 Invasão de computadores

Além do acesso a dados armazenados em provedores através de ordens judiciais, outra tática que está se tornando popular entre órgãos investigativos do mundo todo conforme a adoção de criptografia aumenta nas ferramentas de comunicação *online* é a **invasão de computadores** através de **códigos de exploração de vulnerabilidades, ou exploits**. A invasão pode ser feita uma única vez, para acessar documentos e registros, ou pode instalar um **programa espião / cavalo de tróia** que registra conversas e ações e as manda de volta para seu "dono" através da rede ou em uma subsequente visita ao alvo.

Exploração remota
(invasão)

Acesso legítimo

qual o clima em **[rio de janeiro]**?



mínima 22º, máxima 35º, chuva à tarde

Exploração de vulnerabilidade

EXPLOIT

qual o clima em **['OR''='';&MUDARSENHA:(...)]**?

senha alterada! BEEP BEEP

Exploração local
(programa espião / cavalo de tróia)

11.3.1 Vulnerabilidades e "zero-days"

Quando usamos um computador ou smartphone para navegar na Internet, ler e escrever documentos, trocar mensagens ou ouvir música, o que é exibido na tela é somente a ponta de um gigantesco iceberg – por baixo dos aplicativos abertos e da área de trabalho, milhares de *softwares* feitos de forma independente por organizações e indivíduos ao redor do mundo.

Cada um desses programas se comunica com os outros através de mensagens, encaminhadas pelo *kernel*, o núcleo do sistema, e através da Internet quando se está usando uma aplicação na rede. Quando recebe uma dessas mensagens, um programa extrai o conteúdo dela e "encaixa" em seu algoritmo para decidir o que fazer com isso.

Uma **vulnerabilidade de software** existe quando se pode mandar uma mensagem construída especialmente para confundir o sistema que se quer invadir ("batizada", como diz a expressão popular) e fazê-lo encarar as mensagens recebidas como ordens de comando, ou conceder acesso privilegiado a determinado usuário que já existe no sistema.

Um **exploit**, ou **código de exploração**, é um programa que explora uma vulnerabilidade para conseguir na prática tal acesso ao sistema.

Por serem usadas para cometer crimes – seja fraudes bancárias, roubo de segredos industriais e dados pessoais, falsidade ideológica, fraude, etc – as vulnerabilidades não são desejadas pelos fabricantes de software, que possuem equipes dedicadas a encontrá-los – seja por conta própria, por relatos de incidentes ou através de sistemas de recompensa a pesquisadores – e resolvê-los, mudando o código para remendar a falha e encaminhando atualizações de segurança para os usuários.

O mundo da segurança da informação e dos cibercrimes (e, como vemos, da "interceptação legal") é uma eterna caça de gato e rato entre quem pesquisa vulnerabilidades e quem as conserta, um determinado *exploit* descoberto ou adquirido possui prazo de validade. Vulnerabilidades, quando mantidas por muito tempo em segredo, são descobertas independentemente por outros(as) pesquisadores(as), e quando adquiridas costumam ser vendidas também para outras entidades; uma vez que se dê o uso da vulnerabilidade para invasões se torna questão de tempo até que as empresas de antivírus e segurança da informação detectem a falha e corrijam o *software*.

As vulnerabilidades com status de **zero-days** ("zero dias") são aquelas que ainda não foram descobertas por profissinais de segurança e não ainda não foram usadas contra nenhum alvo (ou estão começando exatamente agora). O nome é uma referência à contagem de dias que levam até que o problema seja corrigido, os possíveis alvos atualizem seus sistemas e a falha não possa mais ser usada tão eficazmente.

Como os *softwares* que usamos vêm tornando sua rotina de atualização mais eficiente e automática, é cada vez mais difícil usar uma vulnerabilidade já "gasta" em novos alvos. A busca por *zero-days* se torna necessária para qualquer operação importante, e consegui-los envolve interagir com um mercado que se encontra, no mínimo, em uma zona cinzenta de legalidade. Há uma divisão moral clássica nos profissionais de segurança da informação: os *whitehats* ("chapéus brancos") são aqueles que pesquisam, descobrem e catalogam vulnerabilidades e vírus para que as empresas antivírus e as fabricantes de software possam consertá-los, e os *blackhats* ("chapéus pretos") usam as falhas que descobrem ou aprendem com outros(as) *blackhats* para cometer fraudes ou vender serviços de invasão e roubo de dados por encomenda. Profissionais

de diferentes chapéus e intenções interagem através de fóruns da Internet e a linha que separa a pesquisa responsável da atividade criminosa por vezes não é clara – há um terceiro grupo, os *grayhats* ("chapéus cinzas") que não se encaixam ou rejeitam a classificação clássica.

Um relatório de 2014 da norteamericana RAND Corporation sobre o mercado negro de vulnerabilidades e serviços de invasão afirma que o preço de um único *zero-day* "varia de alguns milhares de dólares a US$200.000,00 - US$300.00,00, dependendo do grau de severidade da vulnerabilidade, da complexidade do *exploit*, por quanto tempo a vulnerabilidade permanecerá desconhecida, a versão do produto que será comprometido, e o(a) comprador(a). Algumas estimativas chegam até US$ 1 milhão, mas costumam ser tachadas de exageradas" *[RAND-VULNS-2014]* (Página 108).

Vulnerabilidades já conhecidas, que como vimos são menos eficazes, são mais facilmente encontráveis em fóruns e listas de discussão de segurança, e até em mercado como o ExploitHub, que comercializa *exploits* de vulnerabilidades que não são *zero day*. De acordo com matéria do portal de notícias ZDnet e relatórios financeiros da ExploitHub, em 2013 o valor médio de um *exploit* era de US$ 284,06; o valor chega até US$ 1.500,00 *[ZDNET-VULNS-2014]* (Página 109).

11.3.2 Legalidade incerta; riscos garantidos

Uma vez invadido o sistema, as comunicações visadas pela "interceptação" são reveladas junto com fotos, documentos e registros pessoais, e outras comunicações que nada têm a ver com o propósito da investigação. Por se tratar de uma operação feita sem a cooperação de provedores, atravessando todos os mecanismos de autenticação do sistema invadido, não há uma maneira clara de identificar as ações do(a) invasor(a) nem de limitá-las a algum escopo.

Como diz Laura Schertel Mendes, coordenadora do Centro de Direito, Internet e Sociedade – CEDIS-EDB/IDP (grifo nosso):

> Se o STF no RE 418.416/SC já entendeu que a garantia da inviolabilidade de sigilo art. 5°, XII, referia-se à comunicação de dados e não aos dados em si, é porque certamente o cenário dos riscos ao cidadão era bastante diverso tendo em vista as tecnologias então existentes. Afinal, usualmente os dados sofrem maior risco de interceptação durante o processo de comunicação – isto é, no tráfego – e não enquanto eles estão armazenados. Ocorre que com o advento da internet e dos aparelhos pessoais conectados em rede, a constelação de riscos alterou-se radicalmente e os **programas espiões** são o maior exemplo do **risco de acesso clandestino** e de manipulação dos dados armazenados em sistemas pessoais, que na vida moderna, guardam praticamente todas as informações a respeito de seu usuário. Nesse contexto, **a efetividade da garantia constitucional da inviolabilidade do sigilo pressupõe que ela alcance também os dados armazenados em sistemas informáticos pessoais – tais como computadores, smartphones e agendas eletrônicas – cujo acesso passa a ser possível por meio desses programas e que podem acarretar riscos gravíssimos de monitoramento e vigilância ao cidadão sem que ele tome sequer conhecimento a respeito**. *[MENDES-2015]* (Página 111)

Em sua análise "Interceptações e Privacidade", Gilmar Mendes e o Jurandi Borges Pinheiro também vêem com preocupação a utilização indiscriminada de tecnologias de invasão para

acessar dados e comunicações, prática ainda não bem representada no arcabouço legal brasileiro, possa causar danos ao ferir o direito à privacidade (grifos nossos):

> [...] não é porque eventual inovação no campo tecnológico não esteja suficientemente contemplada na legislação em vigor que a garantia constitucional ameaçada fica sem proteção, cabendo ao intérprete, ao lidar com essa realidade, assegurar que o direito fundamental em si, independentemente das garantias a ele inerentes, não seja menosprezado a ponto de negar-lhe efetividade. Talvez seja esse o caminho ao lidarmos com a proteção do direito à privacidade, quando fragilizado por tecnologias que se transmudam da ficção à realidade em velocidade sem precedentes.
>
> Com essas considerações, poderíamos avançar em relação ao tema não mais nos preocupando tanto em contemplar, em textos legais, de modo específico, cada nova tecnologia que surge, mas, sim, com a **reformulação dos modelos de regulação, de forma a estabelecer requisitos mínimos como, por exemplo, crimes passíveis de investigação por tecnologias invasivas, imprescindibilidade de autorização judicial, duração da investigação, forma de registro de dados obtidos, restrições na divulgação dos dados capturados e sistema de acompanhamento do efetivo cumprimento dos requisitos estabelecidos**.
>
> Enfim, seja qual for o cenário tecnológico que nos cerca, não se pode perder de vista que a boa aplicação dos direitos fundamentais de caráter processual, principalmente da proteção judicial efetiva, é que nos permite **distinguir o Estado de Direito do Estado Policial**. O prestígio desses direitos configura também **elemento essencial de realização do princípio da dignidade humana na ordem jurídica**, impedindo, dessa forma, que o homem seja convertido em mero objeto do processo.

CAPÍTULO 12

Créditos

12.1 Redação

Lucas Teixeira é desenvolvedor, administrador de sistemas e pesquisador. Atua como diretor técnico da Coding Rights, sendo editor do Boletim Antivigilância e um dos criadores do projeto Oficina Antivigilância. Guiado pelo espírito comunitário, ele tem experiência de trabalho em projetos colaborativos e voluntários sobre privacidade, liberdade de expressão, software livre, agroecologia e cultura livre. Também tem desenvolvido métodos de oficinas para treinamento em segurança digital, produzido e traduzido guias e plataformas sobre o tópico.

Joana Varon é fundadora e diretora da Coding Rights, advogada e bacharel em Relações Internacionais pela PUC-SP, mestre em Direito e Desenvolvimento pela Escola de Direito de São Paulo da Fundação Getúlio Vargas (FGV-SP) e especializada em direito e novas tecnologias, já atuou como pesquisadora no Cebrap-SP, no Observatório de Inovação e Competitividade da USP e no Centro de Tecnologia e Sociedade da FGV. Nessa trajetória tem trabalhado em pesquisa aplicada para políticas públicas na área de TICS, como enfoque em análises juridico-institucionais para garantir direitos humanos e inovação na era digital.

Paulo Rená é mestre em Direito, Estado e Constituição (UnB). Professor de Direito (Uni-CEUB). Chefe Executivo de Pesquisa do Instituto Beta Para Internet e Democracia - IBIDEM. Atuou no Ministério da Justiça (SAL/MJ) como gestor do projeto de elaboração coletiva do Marco Civil da Internet no Brasil.

12.2 Apoio

Bia Barbosa é jornalista, integrante da Coordenação Executiva do Intervozes e do Fórum Nacional pela Democratização da Comunicação.

12.3 Agradecimentos

Ícones e *cliparts* do Projeto GNOME e do Openclipart.

Guilherme Damasio Goulart e Vinicius Serafim (do podcast Segurança Legal), Gustavo Paiva e o Grupo de Trabalho de Anonimato no Brasil, e a Comunidade Antivigilância.

CAPÍTULO 13

Referências

CAPÍTULO 14

Propostas para o Relatório Final da CPICIBER

(considerada a versão II, de 11/04/2016)

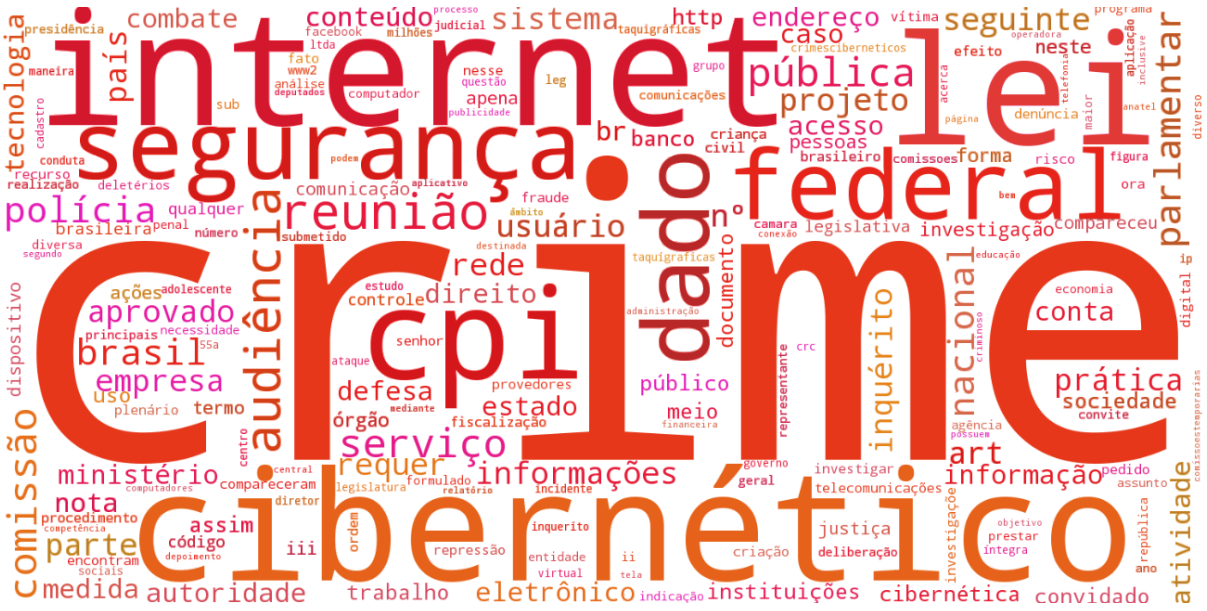


Fig. 14.1: Nuvem de palavras do relatório da CPI. Feita com python e o módulo wordcloud.

Aos deputados relatores da Comissão Parlamentar de Inquérito de Crimes Cibernéticos - CPICIBER.

14.1 Apresentação

Este documento visa oferecer, de forma detalhada, insumos ao Relatório Final da Comissão Parlamentar de Inquérito da Câmara dos Deputados sobre Crimes Cibernéticos - CPICIBER, considerados os termos da segunda versão, divulgada em 11 de abril de 2016. O objetivo é viabilizar o **combate aos cibercrimes** de maneira equilibrada com a **proteção de direitos fundamentais**.

O texto a seguir, elaborado com o propósito de refletir as preocupações diversas e plurais da sociedade civil, é resultado direto do trabalho conjunto das seguintes organizações: Coding

Rights, Instituto Beta: Internet e Democracia (Ibidem), Intervozes – Coletivo Brasil de Comunicação Social e ARTIGO 19.

Objetivamente, oferecemos a seguir **nove propostas** de mudanças, especialmente modificações e supressões nos novos projetos de lei, mas também alterações quanto às indicações e recomendações constantes do texto do relatório final.

Em cada proposta, devidamente numerada, indicamos inicialmente o trecho do relatório final ao qual ela se refere, seguido de um quadro resumo da sugestão de modificação e, por fim, as justificativas correspondentes, pormenorizadas conforme a complexidade das questões.

14.2 Proposta nº 1: Substituir conceitos erroneamente definidos ou irrelevantes

(PARTE II - Constatações e Conclusões > 1 - Introdução > 1.1.3 Conceitos importantes)

NOSSA PROPOSTA

Remover os termos "mail bomb", "worm", "wikileaks", "quebra de senha", "denial of service", "sniffer", "backdoor", "deep web" e "botnets" e acrescentar os seguintes:

Acrescentar os seguintes termos:

- **criptografia**: o estudo das técnicas de se comunicar de forma segura quando se tem alguém escutando o canal de comunicação. Através da criptografia e possível garantir a confidencialidade, a autenticidade e a integridade de mensagens e documentos.
- **criptografia ponta-a-ponta (end-to-end)**: uma maneira de se criptografar mensagens ou arquivos para outras pessoas de forma que somente elas possam acessá-las; as chaves da criptografia ficam armazenadas nos dispositivos, de modo que o provedor de aplicação não pode vê-las.
- **segurança cibernética**: assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas (Estratégia de SIC, GSI/PR, atual Casa Militar).
- **deep web**: compreende todas as páginas web (ou seja, tudo que pode ser acessado pelo navegador) que não estão indexadas e catalogadas nos grandes mecanismos de busca, como Google, Bing e DuckDuckGo. O termo foi inicialmente cunhado para representar a grande parcela da web que não pode ser encontrada nestes portais, indicando que a web é muito maior do que parece à primeira vista – daí a metáfora comum da web "superficial" como a ponta de um iceberg. A deep web obedece ao mesmo ordenamento jurídico que a surface web; não há de fato distinção prática entre sites dentro e fora da deep web para um juiz ou agente.
- **pedofilia**: transtorno psiquiátrico em que um adulto ou adolescente mais velho sente uma atração sexual primária ou exclusiva por crianças pré-púberes, geralmente abaixo dos 11 anos de idade (Wikipédia).

- **abuso sexual de menor:** forma de abuso infantil em que um adulto ou adolescente mais velho usa uma criança ou adolescente mais jovem para estimulação sexual, incluindo a participação em obras de exploração pornográfica infantil.
- **exploração pornográfica infantil:** forma ilegal de pornografia, em que participam crianças e adolescentes.

O Relatório Final, na Introdução da *Parte II - Constatações e Conclusões* (pág. 62), enumera conceitos considerados importantes "*quando se cuida de analisar a Internet e todas as circunstâncias a ela relacionadas*".

Todavia, em 8 páginas do documento, a lista declaradamente compilada "*sem a pretensão, obviamente, de exaurir o tema*", contempla definições escolhidas de forma arbitrária. Muitos dos termos não foram mencionados sequer uma vez nas audiências da CPICBER.

Uma pesquisa por termos, feita a partir das notas taquigráficas de todas as reuniões até o Seminário do dia 29 de março, permitiu elaborar a seguinte tabela, em que se comparam os termos sem definição e aqueles constantes da lista de conceitos do Relatório Final:

"Conceitos importantes" do relatório #CPICIBER			
Não estão definidos		Estão definidos	
termo	**menções**	**termo**	**menções**
cibernética / ciber-	1137	deface	3
criptografia / criptograf-	263	spyware	3
pedofilia	238	Wikileaks	3
privacidade	225	worm	1
anonimato / anonim-	156	hoax	0
pornografia infantil	152	mail bomb	0
segurança da informação	138	sniffer	0

14.3 Proposta nº 2: Redação mais precisa no Art. 154-A do Código Penal

(PARTE III - Proposições e Recomendações > 1 - Projetos de Lei > 1.2 Projeto de Lei para alterar a redação do art. 154-a do Decreto-Lei no 2.848, de 7 de dezembro de 1940, para ampliar a abrangência do crime de invasão de dispositivo informático)

NOSSA PROPOSTA

Alterar a redação do Projeto de Lei proposto pelo Relatório, da seguinte maneira:

Forma final:

> Art. 2º O artigo 154-A do Decreto-Lei no 2.848, de 7 de dezembro de 1940, passa a vigorar com a seguinte redação:

Art. 2º O artigo 154-A do Decreto-Lei no 2.848, de 7 de dezembro de 1940, passa a vigorar com a seguinte redação:

~~Invasão de~~ **Acesso indevido a** dispositivo informático

Art. 154-A. ~~Invadir~~ **Acessar indevidamente** dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou **com o fim de** instalar vulnerabilidades para obter vantagem ilícita:

Acesso indevido a dispositivo informático

Art. 154-A. Acessar indevidamente dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou com o fim de instalar vulnerabilidades para obter vantagem ilícita:

Quais condutas exatamente se buscam tipificar e que já não estejam previstas no atual art. 154-A do Código Penal, que trata da finalidade de "*obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita*"?

O tipo penal atualmente em vigor, apesar de conter problemas, mostra-se mais equilibrado que a redação proposta, pois define a conduta de forma mais restrita, impedindo o enquadramento de condutas que não sejam o alvo específico da proteção jurídica em questão.

A alteração proposta pelo relator na segunda versão do projeto de lei, com vistas a superar as críticas de que a redação seria muito vaga, não resolve o problema. A expressão "*acesso indevido*", combinada ao restante do tipo penal proposto, mantém o caráter genérico, podendo abarcar uma variedade de condutas não necessariamente ilícitas ou prejudiciais. Por exemplo, legítimas investigações de segurança, que não ocorreriam em um ambiente de exigência de autorização, seriam criminalizadas no texto proposto pelo relator, mas não na nossa sugestão.

Consideramos especialmente vago o trecho "*expondo os dados informatizados a risco de divulgação ou de utilização indevidas"*. O termo "risco" torna inexigível haver efetiva divulgação ou a utilização indevida dos dados. Mas o quê exatamente caracteriza esse risco? Basta acessar ou armazenar os dados?

A ausência de uma definição para o significado de "risco" se agrava porque associada à expressão "*utilização indevida*". No limite, qualquer acesso a um sistema informatizado ou a dispositivo informático pode expor os dados a risco de "*divulgação ou de utilização indevidas*".

O dolo e o real risco de dano se demonstram mais concreta e adequadamente na delimitação de que o crime ocorre quando o acesso ocorre "*sem a autorização expressa ou tácita do titular do dispositivo*". A menção ao titular é um elemento do tipo fundamental, presente também na expressão vigente "*dispositivo informático alheio*".

Um dos postulados ínsitos ao princípio da legalidade no direito penal é o princípio da taxativi-

dade (*lex certa*), segundo o qual o tipo penal deve ser claro, preciso e determinado, permitindo ao cidadão a real consciência acerca da conduta punível criminalmente pelo Estado.

Defendemos a manutenção da maior parte do art. 154-A atualmente vigente. Concordamos, porém, que se substitua "invadir" por "*acessar indevidamente*", termo mais adequado do ponto de vista da redação técnico-jurídica, pois não se trata de coibir a *invasão,* tomada como a entrada presencial de alguém em algum lugar, mas apenas de vedar um acesso virtual.

Ressalte-se, como já dito, que esse termo ficará vago e impreciso se não vier acompanhado de todas as delimitações atualmente presentes no texto do Código Penal.

14.4 Proposta nº 3: Substituir utilização do Fistel pela utilização do FNSP

(PARTE III - Proposições e Recomendações > 1 - Projetos de Lei > 1.3 – Projeto de Lei visando à alteração da Lei nº 5.070, de 7 de julho de 1966, para autorizar o uso dos recursos do Fistel por órgãos da polícia judiciária)

NOSSA PROPOSTA

Não alterar o art. 5º da Lei nº 5.070/1966, que trata do FISTEL – Fundo de Fiscalização das Telecomunicações, mas sim o art. 4º da Lei nº 10.201/2001, que regula o FNSP – Fundo Nacional de Segurança Pública, nos seguintes termos:

> Art. 2º O artigo 4º da Lei nº 10.201, de 14 de fevereiro de 2001, passa a vigorar acrescido do seguinte parágrafo:
>
> > Art. 4º .....
> > .....
> >
> > § 9º. Até 10 % (dez por cento) das transferências para o Tesouro Nacional poderão ser utilizados pelos órgãos da polícia judiciária de que trata o artigo 4o da Lei nº 12.735, de 30 de novembro de 2012. (NR)
>
> Art. 3º Esta lei entra em vigor um ano após sua publicação oficial.

A proposta de PL a ser alterada é escrita, justificada e mencionada nos seguintes trechos do relatório final:

- Item 2.4.4 – "Alocação de recursos do Fistel – Fundo de Fiscalização das Telecomunicações – para manutenção das polícias especializadas" da sub-relatoria de Segurança Cibernética no Brasil, do deputado Rodrigo Martins (pág 134).
- Item nº 14 das Conclusões do Relator, deputado Espiridião Amin (pág 164).
- Projeto de Lei nº 1.3 – "visando à alteração da Lei n o 5.070, de 7 de julho de 1966, para autorizar o uso dos recursos do Fistel por órgãos da polícia judiciária" (pág 178).

Sem dúvida, o Estado precisa se aprimorar para combater de forma específica os cibercrimes. Entretanto, esse objetivo não pode ser alcançado mediante um desvio de finalidade do FISTEL

- Fundo de Fiscalização das Telecomunicações.

Especialmente quando existe o **Fundo Nacional de Segurança Pública - FNSP** (criado pela Lei nº 10.201/2001), com previsão legal específica para esse propósito, com a expressa exigência de compromisso com resultados, enumeração de órgãos que podem ter acesso aos recursos, definição de prazo de realização, e disciplina de forma e condições de aplicação:

> **Art. 1º** Fica instituído, no âmbito do Ministério da Justiça, o Fundo Nacional de Segurança Pública – FNSP, com o objetivo de apoiar projetos na área de segurança pública e de prevenção à violência, enquadrados nas diretrizes do plano de segurança pública do Governo Federal. (Redação dada pela Lei nº 10.746, de 10.10.2003)
>
> (...)
>
> **Art. 4º** O FNSP apoiará projetos na área de segurança pública destinados, dentre outros, a: (Redação dada pela Lei nº 10.746, de 10.10.2003
>
> **I** - reequipamento, treinamento e qualificação das polícias civis e militares, corpos de bombeiros militares e guardas municipais; (Redação dada pela Lei nº 10.746, de 10.10.2003)
>
> **II** - sistemas de informações, de inteligência e investigação, bem como de estatísticas policiais; (Redação dada pela Lei nº 10.746, de 10.10.2003)
>
> **III** - estruturação e modernização da polícia técnica e científica; (Redação dada pela Lei nº 10.746, de 10.10.2003)
>
> (...)
>
> **V** - programas de prevenção ao delito e à violência. (Redação dada pela Lei nº 10.746, de 10.10.2003)

Por sua vez, os recursos do FISTEL, disciplinados pela Lei nº 5.070/1966 (com redação dada pela Lei nº 9.472/1997), têm previsão clara de aplicação exclusiva para a fiscalização de serviços de telecomunicações.

> **Art. 1º**. Fica criado um fundo de natureza contábil, denominado "Fundo de Fiscalização das Telecomunicações", destinado a prover recursos para cobrir despesas feitas pelo Governo Federal na execução da fiscalização de serviços de telecomunicações, desenvolver os meios e aperfeiçoar a técnica necessária a essa execução.
>
> **Art. 3º** Além das transferências para o Tesouro Nacional e para o fundo de universalização das telecomunicações, os recursos do Fundo de Fiscalização das Telecomunicações - FISTEL serão aplicados pela Agência Nacional de Telecomunicações exclusivamente: (Redação dada pela Lei nº 9.472, de 1997)
>
> > **a)** na instalação, custeio, manutenção e aperfeiçoamento da fiscalização dos serviços de telecomunicações existentes no País;
> >
> > **b)** na aquisição de material especializado necessário aos serviços de fiscalização;
> >
> > **c)** na fiscalização da elaboração e execução de planos e projetos referentes às telecomunicações;

> **d)** no atendimento de outras despesas correntes e de capital por ela realizadas no exercício de sua competência. (Incluído pela Lei nº 9.472, de 1997)

Em primeiro lugar, mostra-se necessário esclarecer que conexão à Internet não é propriamente um serviço de telecomunicação, mas sim um serviço de **valor adicionado**, conforme definição vigente da Norma 04/1995 do Ministério da Comunicações, que regulamenta de forma específica "*o uso de meios da Rede Pública de Telecomunicações para o provimento e utilização de Serviços de Conexão à Internet*". Por essa norma, a conexão à Internet é considerada juridicamente como um serviço que acrescenta a uma rede de telecomunicações preexistente os meios ou recursos que criam novas utilidades específicas, ou novas atividades produtivas, relacionadas com o acesso, armazenamento, movimentação e recuperação de informações.

Logo, o acesso a um serviço *online* é só um uso particular de um serviço de telecomunicação (telefonia fixa, móvel, TV por assinatura, redes de banda larga), mas não se confunde com ele. Portanto, não pode ser alvo de fiscalização apoiada em investimentos de recursos do FISTEL, o qual, repita-se, destina-se exclusivamente à fiscalização de serviços de telecomunicações.

Há tantos problemas na atuação das operadoras de telecomunicações, as quais sempre estão no topo das listas de reclamações dos consumidores, que não faz sentido redirecionar para outros propósitos os recursos de um fundo destinado a fiscalizar esses serviços e, por esse meio, contribuir ao aprimoramento de sua qualidade. Em especial quando os constantes contingenciamentos do fundo prejudicam a própria Anatel no exercício de sua função, como alerta a recomendação do Ministério Público Federal feita à Presidência da República e a Ministérios ao final de 2014.

A utilização do FISTEL por órgãos da polícia judiciária agravaria esses problemas, por insistir na alocação dos recursos em finalidade estranha aos objetivos do fundo, que já não vêm sendo cumpridos a contento. Ainda mais grave, a proposta do relatório da CPICIBER redireciona seus fundos para a vigilância dos usuários de Internet, majoritariamente ocupados em atividades lícitas e que, repita-se, não se enquadram sequer como serviço de telecomunicação.

Nesse cenário, não se mostra justificável transferir parte do FISTEL para equipar a polícia no combate a crimes cibernéticos por meio de uma falaciosa "fiscalização" dos usuários. Não há problema em equipar mais e melhor a polícia, mas os recursos devem vir de fontes adequadas, já existentes, como o citado FNSP, sem prejudicar outras finalidades.

Logo, mesmo que se considere a possibilidade real de usos da Internet que não observem a legalidade, o propósito dos maiores investimentos nesse momento deve estar voltado para o fomento do uso da Internet, a partir de sua finalidade social. Investimentos em redes de banda larga podem contribuir e muito para a qualidade dos serviços de telecomunicações. Também por isso o governo federal vem trabalhando com a possibilidade de aplicar o FISTEL no financiamento de suas políticas de acesso à banda larga, o que novamente não pode ser desprezado na análise desse projeto de lei. Como disse Tim Berners-Lee, inventor da Web, em sua Carta Aberta aos Legisladores Brasileiros:

> Sugestões de que o dinheiro destinado a conectar mais brasileiros seja realocado para fundos de policiamento da rede são iniciativas difíceis de se entender, ainda mais quando quase metade do país ainda não pode se beneficiar de um acesso à Internet com frequência.

14.5 Proposta nº 4: Regras para indisponibilização de conteúdo infringente idêntico

(PARTE III - Proposições e Recomendações > 1 - Projetos de Lei > 1.5 – Projeto de Lei determinando a indisponibilidade de cópia de conteúdo reconhecido como infringente, sem a necessidade de nova ordem judicial e dá outras providências)

NOSSA PROPOSTA

Alterar a redação do Projeto de Lei proposto pelo Relatório, da seguinte maneira:

Art. 1º Esta Lei modifica o Marco Civil da Internet, Lei n o 12.965, de 23 de abril de 2014, determinando a indisponibilidade de cópia de conteúdo reconhecido como infringente, sem a necessidade de nova ordem judicial e dá outras providências.

Art. 2º A Lei nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet, passa a vigorar acrescida dos seguintes dispositivos:

> Art. 19-A Quando se tratar ~~Art. 21 A Os provedores aplicação deverão tomar as providências técnicas, tendo em conta o conjunto~~ de cópia de ~~meios suscetíveis~~ conteúdo infringente que já tenha sido objeto de ordem judicial determinando sua indisponibilização, o provedor de ~~serem razoavelmente utilizados~~ aplicação, no âmbito e nos limites técnicos de ~~suas aplicações, para assegurar~~ seu serviço, de forma diligente, deverá torná-la indisponível sempre que ~~o conteúdo infringente, objeto da ordem judicial ou da~~ houver nova notificação ~~de~~ que ~~trata esta Seção, continue indisponível em caso de cópia, dispensada~~ aponte a ~~necessidade de nova ordem~~ localização inequívoca da cópia e a decisão judicial ~~ou notificação para~~ que fundamenta a ~~retirada desses novos materiais.~~ sua indisponibilização.
>
> **Parágrafo único.** Para os efeitos deste artigo, é considerada cópia o conteúdo idêntico ao original ~~ou que contenha parte majoritária do conteúdo original~~ e que continue a configurar a característica considerada como infringente;

Íntegra de nossa proposta do novo Art. 19 sem marcações de mudanças:

> **Art. 1º** Esta Lei modifica o Marco Civil da Internet, Lei n o 12.965, de 23 de abril de 2014, determinando a indisponibilidade de cópia de conteúdo reconhecido como infringente, sem a necessidade de nova ordem judicial e dá outras providências.
>
> **Art. 2º** A Lei nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet, passa a vigorar acrescida dos seguintes dispositivos:
>
> > **Art. 19-A** Quando se tratar de cópia de conteúdo infringente que já tenha sido objeto de ordem judicial determinando sua indisponibilização, o provedor de aplicação, no âmbito e nos limites técnicos de seu serviço, de forma diligente, deverá torná-la indisponível sempre que houver nova notificação que aponte a localização inequívoca da cópia e a decisão judicial que fundamenta a sua indisponibilização.
> >
> > **Parágrafo único.** Para os efeitos deste artigo, é considerada cópia o conteúdo idêntico ao original que continue a configurar a característica considerada como infringente;

Concordamos que não faz sentido exigir novas ordens judiciais e, portanto, a proposição de novas ações, a fim de que se indisponibilizem conteúdos já considerados infringentes pelo Poder Judiciário. Tratando-se de cópia de conteúdo já submetido ao crivo judicial e considerado ilícito, a indisponibilização pode se dar por meio de mera notificação do interessado, desde que a notificação permita a localização inequívoca do material (conforme exigência do art. 19, §1º, do Marco Civil da Internet - Lei nº 12.965/2014) e aponte a decisão que o reputou infringente.

As hipóteses de responsabilização dos provedores de aplicações por descumprimento de mera notificação são excepcionais no Marco Civil da Internet. O objetivo dessa norma é equilibrar a garantia da liberdade de expressão e do acesso à informação com a proteção de outros direitos no ambiente *online*, entre eles a honra, a imagem, o nome etc.. A figura institucional competente para avaliar tal equilíbrio é o juiz, cuja imparcialidade e o saber jurídico são necessários para decidir o conflito de interesses nas controvérsias sobre indisponibilização de conteúdo online.

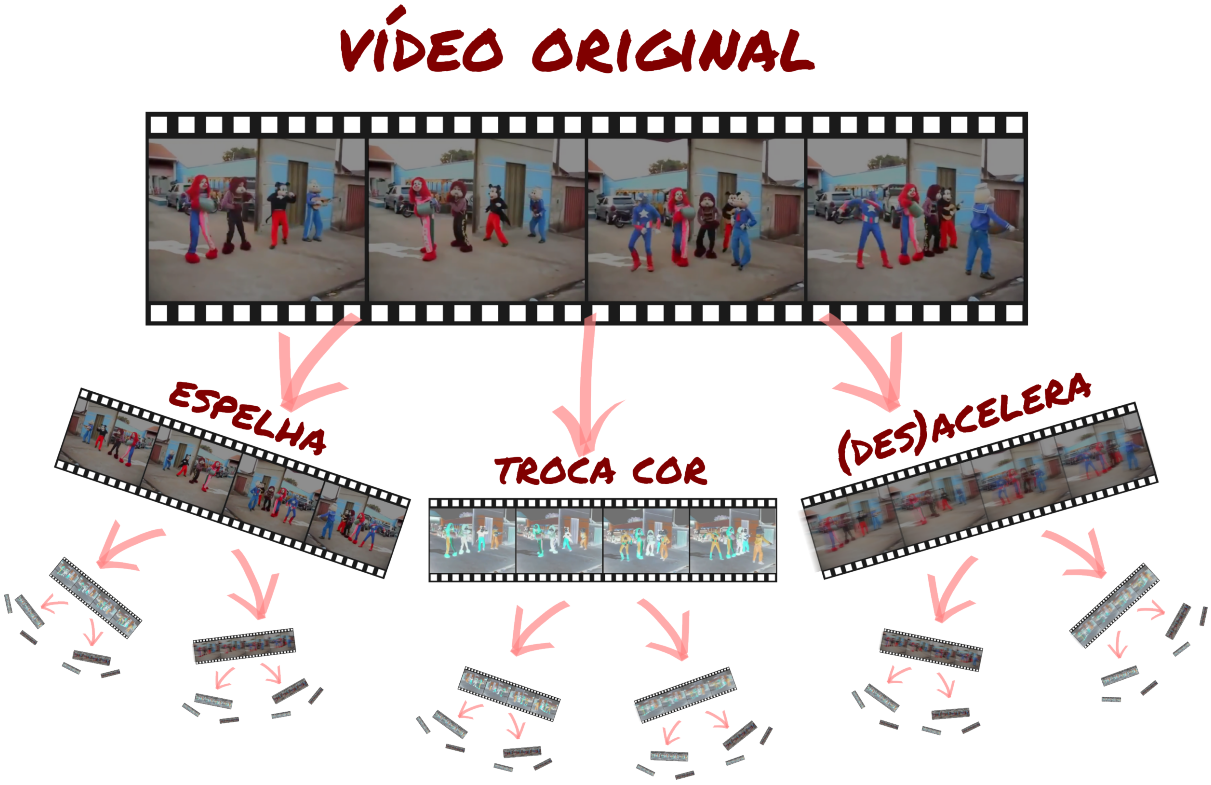
Esse papel não pode ser conferido ao provedor de aplicações, que em geral tenderá a seguir, por interesses econômicos, o caminho da segurança jurídica, retirando sempre os conteúdos, como forma de evitar processos judiciais e o pagamento de indenizações. Essa via abriria larga margem para a censura online. Por sua vez, a regra geral do Marco Civil é a responsabilização dos provedores de aplicações pelos conteúdos de terceiros apenas se aqueles intermediários descumprem ordem judicial que determinou a indisponibilização. Entretanto, a sugestão posta no relatório final insere no Marco Civil nova hipótese de notificação e retirada ("notice and takedown"), em lógica incompatível com a regra geral.

Cria, portanto, uma antinomia, por não observar a norma do § 1º do art. 19, que exige, para validade da ordem judicial, a "*identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material*".

Além disso, a proposta do relatório, ao criar uma dinâmica de constante monitoramento dos conteúdos pelo provedor de aplicações, se mostra perigosa e complexa. Sendo possível desenvolver ferramentas automáticas de identificação de conteúdo, a medida poderia parecer de exigência razoável em relação às grandes aplicações online, como Facebook. Mas a maior parte dos sites e aplicativos, por sua estrutura reduzida, teria grande dificuldade para investir na operação de ferramentas desse tipo. A obrigatoriedade significaria uma relevante barreira à entrada, impactando negativamente na inovação na rede.

No entanto, as dificuldades não param aqui e podem atingir mesmo as grandes empresas. Conforme Pedro Markun, em audiência realizada por esta CPI, na identificação de "conteúdos repetidos", é comum que vídeos bloqueados sejam relançados na rede com pequenas alterações como espelhar a imagem (*flipar*, como diz Markun), mudar a velocidade de reprodução ou mudar sutilmente as cores da imagem. Com a combinação de algumas destas modificações já é possível produzir exponencialmente variantes que são, no mínimo, um grande desafio para técnicas de identificação de conteúdo repetido como PhotoDNA e *hashing*, mencionadas na CPI. Mesmo que a aplicação disponha desses mecanismos de identificação, técnicas como as mencionadas acima podem fazer com que o mecanismo falhe nessa identificação e o provedor de aplicações seja responsabilizado sem que tenha havido de fato dolo, ou mesmo culpa, na manutenção de conteúdo já considerado infringente.

Por isso, apresentamos como sugestão a solução de indisponibilizar a cópia de conteúdo medi-



ante mera notificação. Com isso, não queremos que o ônus de "procurar o conteúdo" passe à vítima, mas acreditamos que o usuário afetado, melhor do que qualquer outro agente, terá conhecimento dos links que o ofendem e poderá reportá-los sem grande burocracia ao provedor de aplicações, que deverá indisponibilizá-los o mais rápido possivel, no âmbito e nos limites técnicos de seu serviço, sem necessidade de ordem judicial. Do contrário, estaríamos colocando os sites e aplicativos na posição de eternos vigias de conteúdo na Internet, o que causaria sérios impactos à sua atividade e mesmo aos usuários de forma geral, mais monitorados em relação às suas postagens. Nossa proposta visa compatibilizar a preocupação do relator à proteção da livre iniciativa, da livre concorrência, da liberdade de expressão e do acesso à informação. Por fim, justificamos outros três pontos que merecem atenção:

1. Considerando a redação proposta e o objeto mais amplo, atinente à responsabilização civil, após ordem judicial específica, por danos decorrentes de conteúdo gerado por terceiros, mostra-se mais adequado o novo artigo ser numerado como 19-A e não 21-A.

2. Buscando precisão terminológica, a proposta ora apresentada se exclusivamente do termo "indisponibilização", sem fazer referência ao termo "retirada". Tanto do ponto de vista teórico jurídico, quanto pela perspectiva prática tecnológica, "*retirar um conteúdo*" da Internet não é o mesmo que "tornar indisponível o acesso". O Marco Civil da Internet já se refere à "indisponibilização de conteúdo", reforçando ser essa a terminologia adequada.

3. Na definição de cópia mantemos apenas os casos de "cópia idêntica", isso porque a expressão "parte majoritária" constitui um termo vago, que replicaria no texto do Marco Civil um dos grandes problemas na legislação de direito autoral, que considera legal a utilização pessoal de "pequenos trechos" de obras intelectuais (art. 46, II, da Lei nº 9.610/1998) e até hoje se demonstra como baliza de controversa aplicação prática. Não é incomum que conteúdos na Internet sejam parcialmente replicados com sentidos dife-

rentes, sem que nesse novo contexto sejam considerados ofensivos. Pequenas alterações podem levar a isso e, novamente, não deve caber ao provedor de aplicações decidir se, após a alteração, o conteúdo continua infringente ou não.

14.6 Proposta nº 5: Não permitir o acesso ao endereço IP sem ordem judicial

(Parte III - Proposições e Recomendações > 1 - Projetos de Lei > 1.2 – Projeto de Lei para alterar a redação do art. 154-a do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, para ampliar a abrangência do crime de invasão de dispositivo informático)

NOSSA PROPOSTA

Remover Projeto de Lei que "permite que a autoridade de investigação requisite, independentemente de autorização judicial, o endereço IP utilizado para a geração de conteúdo específico objeto de investigação criminal, mantidos por provedor de conexão ou de aplicação de internet".

O PL é justificado e mencionado nos seguintes trechos:

- Item 2.3.2 – "Acesso ao endereço IP utilizado para a geração de conteúdo específico objeto de investigação criminal" da sub-relatoria de Crimes Contra a Honra e Outras Injúrias, do deputado Daniel Coelho (pág 128).
- Item nº 11 das Conclusões do Relator, deputado Espiridião Amin (pág 164).
- Projeto de Lei nº 1.6 – "permitindo que a autoridade de investigação requisite, independentemente de autorização judicial, endereço IP que identifique conteúdo ou serviço específico, objeto de investigação criminal, mantidos por provedor de conexão ou de aplicação de Internet" (pág 190).

Primeiramente, a parte final do *caput* do art. 1º incorre em um erro conceitual, ao considerar a possibilidade de um "provedor de conexão" manter um conteúdo específico objeto de investigação criminal. Talvez a redação estivesse direcionada a permitir que a requisição pudesse ser feita a esse provedor, mas o texto proposto não alcança essa suposta finalidade.

Não obstante, em um contexto no qual o conteúdo investigado seja conhecido, permitir que a autoridade de investigação requisite, independentemente de autorização judicial, o endereço IP utilizado equivale a requisitar o próprio registro de acesso, cuja disponibilização deve ser sempre precedida de autorização judicial, conforme os arts. 10, § 1º, 15, § 3º, 22 e 23 do Marco Civil da Internet.

A permissão de qualquer acesso a dados pessoais de cidadãos sem ordem judicial não tem paralelo em legislações de países democráticos, os quais somente assim são considerados na medida em que respeitem precisamente as garantias fundamentais que estruturam um Estado de Direito. Direitos humanos não podem ser fragilizados a pretexto de atender à celeridade de uma investigação, por um procedimento que, na prática, pode significar uma porta aberta a arbitrariedades e a violações de direitos. Destaque-se que a previsão de eventual punição para

o mau uso de dados pessoais não tem o condão de reparar o prejuízo decorrente da ofensa a uma garantia constitucional, notadamente se realizada de forma sistemática e em massa.

E embora a Polícia Civil seja menos conhecida do que a Polícia Militar por abusos e corrupção, a instituição conta com seus próprios escândalos: há poucos meses o inspetor-chefe da Corregedoria da Polícia Civil foi afastado do cargo por envolvimento "em acusações de favorecimento e tráfico de influência", acusações que enfrenta junto a seis corregedores, segundo matéria da Agência Brasil. Um vídeo em matéria do Estadão mostra dois policiais civis fugindo de promotores que iriam prendê-los no DEIC/SP sob acusação de receber propina em troca de vista grossa; é possível que a própria corregedoria, convocada pelos promotores para acompanhá-los, tenha avisado os policiais.

De acordo com dados da Ouvidoria de Polícia de São Paulo, entre 1998 e 2014 houve 591 delegados investigados a partir de denúncias na Ouvidoria, que resultaram em 144 punições; houve também 10 investigações contra "agentes de telecomunicações", com 4 policiais punidos. Sem desmerecer o importante trabalho de agentes policiais honestos, conceder acesso a dados sem ordem judicial, como o endereço IP no caso do Projeto de Lei sendo proposto, irá fatalmente gerar abusos.

Em resumo, a proposta cria uma antinomia, em burla à garantia, expressa no Marco Civil, de que depende sempre de ordem judicial a disponibilização dos registros de conexão e dos registros de acesso a aplicações de Internet. Trata-se de um direito específico que dá conteúdo ao devido processo legal, alcançado mediante um consenso legislativo, resultado de um amplo debate que culminou na Lei nº 12.965/2014, cuja importância democrática e precisão técnica não deveria ser desprezada pela CPI.

14.7 Proposta nº 6: Não permitir bloqueio de aplicações

(PARTE III - Proposições e Recomendações > 1 - Projetos de Lei > 1.7 - Projeto de Lei que possibilita o bloqueio de aplicações de Internet por ordem judicial)

NOSSA PROPOSTA

Retirar a proposta de que os provedores de conexão sejam colocados na posição de monitoramento de aplicações.

O bloqueio de páginas da Internet com a justificativa de proteção a direitos autorais é uma restrição desproporcional à liberdade de expressão, devido aos riscos associados de excesso de bloqueio e à falta geral de eficácia dessa medida. Mesmo em relação aos direitos de crianças e adolescentes o problema permanece, contrapondo esses dois riscos - o excesso de bloqueio, por um lado, e a eficácia duvidosa, por outro.

Embora o bloqueio de páginas da Internet seja colocado como último recurso a ser adotado, é muito claro que o expediente será usado de maneira abusiva e desproporcional tendo em vista, por exemplo, recentes decisões de bloqueio do aplicativo Whatsapp, que levou à detenção do vice-presidente para a América Latina do Facebook.

O juiz poderá determinar o bloqueio da aplicação inteira, deixando fora do ar um grande conjunto de conteúdos lícitos e legítimos, podendo, inclusive, prejudicar a comunicação dos usuários da rede de forma geral, como ocorreu com o Whatsapp ou poderia ocorrer se o Gmail ou Yahoo fossem bloqueados, por exemplo.

Ainda, embora a proposta tenha surgido mais especificamente de preocupações relacionadas com direitos autorais e direitos de crianças e adolescentes, a autorização inserida no art. 9º do Marco Civil da Internet é genérica o suficiente para abarcar quaisquer outras hipóteses que envolvam uma conduta criminosa e que o site ou aplicativo não estejam cumprindo a ordem judicial.

É certo que as aplicações devem respeitar as determinações do Judicário e as legislações processuais, cível e penal, já contêm instrumentos suficientes para dar efetividade à atividade jurisdicional. Prever essa autorização geral de bloqueio de aplicações no Marco Civil da Internet dá mais margem a abusos do que, de fato, resolve o problema que se quer atacar.

Em relação a conteúdo ofensivo, por exemplo, é notória a ineficiência da medida, uma vez que bloqueada uma página, surgem outras inúmeras exatamente com o mesmo conteúdo dada a natureza da rede. Sem mencionar que muitos conteúdos protegidos por direitos autorais não são compartilhados em uma plataforma específica, mas parcialmente compartilhados entre pares. Ainda pior, ordens de bloqueio para impedir futuras violações de direitos são uma forma de censura prévia.

Por fim, o bloqueio de sites fere a neutralidade de rede, um dos principais direitos garantidos pelo Marco Civil da Internet. A fim de cumprir a ordem judicial, provedores de conexão a internet serão obrigados a vasculhar os pacotes de dados com o objetivo de encontrar o conteúdo infrigente ou impedir o acesso a ele. É um precedente bastante perigoso que pode ensejar que a técnica seja usada com fins comerciais e outros interesses.

14.8 Proposta nº 7: Não ampliar o acesso ao cadastro de usuários de telefones pré-pagos

(PARTE III - Proposições e Recomendações > 2 – Propostas de Fiscalização e Controle > 2.1 - Propõe que a Comissão de Ciência e Tecnologia, Comunicação e Informática, fiscalize, com auxílio do Tribunal de Contas da União – TCU, as ações de acompanhamento e controle da Agência Nacional de Telecomunicações – ANATEL acerca da correta implementação e utilização dos cadastros de usuários de telefones pré-pagos)

(Fiscalização do cadastro de acesso à Internet em celulares pré-pagos)

NOSSA PROPOSTA

Remover proposta de fiscalização do controle da ANATEL sobre cadastros de usuários de telefones pré-pagos.

A proposta é mencionada nos seguintes trechos:

- Item 2.4.5 – "Fiscalização por parte do TCU das ações da Anatel no que diz respeito ao cadastro dos acessos pré-pagos à internet" da sub-relatoria de Segurança Cibernética no

Brasil, do deputado Rodrigo Martins (pág 135).

- Item nº 15 das Conclusões do Relator, deputado Espiridião Amin (pág 164).
- Proposta de fiscalização e controle nº 2.1 – "propõe que a Comissão de Ciência e Tecnologia, Comunicação e Informática, fiscalize, com auxílio do Tribunal de Contas da União – TCU, as ações de acompanhamento e controle da Agência Nacional de Telecomunicações – ANATEL acerca da correta implementação e utilização dos cadastros de usuários de telefones pré-pagos" (pág 199).

A mera existência de um cadastro de usuários de telefone pré-pago é problemática. Incluir novos atores públicos na gestão desse banco de dados fragiliza a privacidade e a liberdade de expressão, sem que se conheça publicamente indícios empíricos quaisquer de que a atividade polícia tenha tido sucesso no combate ao crime mediante tal ferramenta.

Vale aduzir que o art. 5º, XII, da Constituição Federal veda o anonimato no âmbito da "*liberdade de manifestação do pensamento*". Assim, (i) o anonimato é vedado apenas para se expressar, mas não para acessar informação, o que corresponde a "ir e vir" nas redes; e (ii) a proibição ao anonimato deve ser flexibilizada quando se verificar que se trata de uma condição necessária à própria manifestação individual, o que pode ocorrer mesmo em um contexto democrático, por exemplo, nos mecanismos de denúncia anônima e no e sigilo de fonte jornalística.

O anonimato não se confunde, por si só, com a efetiva prática de um crime. Sugerimos expressamente a reinterpretação e proteção do anonimato como forma de exercício do direito humano de acesso à informação, virtual ou presencial, mas também como mecanismo de segurança para opiniões e expressão de ideias contra eventuais ataques arbitrários e ilegais.

Por sua vez, a privacidade deve ser entendida como o direito que cada pessoa tem de traçar, sobre a sua própria vida, a linha que separa a porção compartilhada e a parte reservada. Ela constitui uma escolha livre e individual, de acordo com suas próprias convicções e forma de ver o mundo. Uma garantia de que é possível ter uma vida privada. Nesse conceito amplo, a privacidade vai muito além do ditado "quem não deve não teve". Não se trata de um temor contra a revelação de segredos, de um medo de que aspectos obscuros sejam conhecidos. Pensar assim levaria à conclusão de que seria necessário ter feito algo errado para ter direito à privacidade, um contrassenso cruel no qual justamente as pessoas que se portam corretamente seriam punidas com a redução da proteção sobre a própria vida.

A privacidade não é uma defesa para criminosos, nem uma cobertura para condutas erradas. É uma garantia de liberdade, para preservar a individualidade das pessoas, nos termos em que elas mesmas quiserem. Do conforto do lar ao ambiente de trabalho, passando pelo uso de um celular pré-pago, o que importa é ter a opção sobre abrir ou fechar porta do quarto, sobre revelar ou não o valor do seu contracheque, sobre vincular ou não o CPF a um número de telefone, sem nenhuma imposição, e com a segurança de que não haverá desrespeito.

Consideradas a ressignificação da vedação ao anonimato, e firme na defesa da privacidade, é necessário concluir que se a legislação em vigor exige que a ANATEL mantenha um cadastro de usuários de telefones pré-pagos, o risco de vazamento de dados ou acesso abusivo apenas aumenta caso se submeta esse banco de dados ao escrutínio da Comissão de Ciência e Tecnologia, Comunicação e Informática da Câmara dos Deputados, com auxílio do Tribunal de Contas da União.

Sem desmerecer os nobres propósitos da proposta, tampouco ignorando a lisura e seriedade das instituições legislativas, o fato é que a própria comunicação desses dados entre diversas pessoas permitiria incontáveis portas inadequadas de acesso ao cadastro, com consequências graves de dimensões incalculáveis para milhões de inocentes, que nem mesmo poderiam se proteger adequadamente contra qualquer incidente.

14.9 Proposta nº 8: Não indicar à ANATEL a adoção do IPv6

(Parte III - Proposições e Recomendações > 3 - Indicações > 3.5 - Indicação à Agência Nacional de Telecomunicações, sugerindo a adoção das medidas necessárias para a implantação do IPv6 no país)

NOSSA PROPOSTA

Remover Indicação à Anatel para a implantação do IPv6 ou de tecnologia similar.

A indicação é mencionada nos seguintes trechos:

- Item 2.4.2 – "Guarda dos registros de conexão por todos os provedores de internet e migração para o IPv6 ou tecnologia similar" da sub-relatoria de Segurança Cibernética no Brasil, do deputado Rodrigo Martins. (pág 137);
- Item nº 13 das Conclusões do Relator, deputado Espiridião Amin (pág 163).
- Indicação nº 3.6 – "indicação à Agência Nacional de Telecomunicações, sugerindo a adoção das medidas necessárias para a implantação do IPv6 ou tecnologia similar no país" (pág 250).

Não se sustenta a recomendação, direcionada à ANATEL - Agência Nacional de Telecomunicações, de que o IPv6 seja adotado como instrumento para identificar pessoas mais facilmente, a partir dos registros de conexão à Internet e registros de uso de aplicação *online*.

Primeiro porque a ANATEL, como reguladora de serviços de telecomunicações, nem sequer ostenta competência administrativa sobre o tema. Repita-se que a conexão à Internet não é propriamente um serviço de telecomunicação, mas um **serviço de valor adicionado**, conforme definição vigente da Norma 04/1995 do Ministério das Comunicações. Portanto, não caberia à ANATEL essa atribuição de acelerar a implementação do IPv6.

Segundo, sabe-se que a retenção de dados indiscriminada viola direitos fundamentais como a privacidade e a liberdade de expressão, conforme defendido por diversos representantes da academia e da sociedade civil presentes nesta CPI, bem como pela Corte Interamericana de Direitos Humanos, pela Corte de Justiça Europeia e por Relatores Especiais da ONU. Não há estatísticas ou estudos que justifiquem esse caminho, mas apenas ilações anedóticas nas falas de delegados e outros representantes de setores policiais ou investigativos.

Terceiro, há um problema prático na adoção do IPv6 como meio de identificação de usuários. O Relatório Final pressupõe que o novo sistema permitiria superar a dificuldade do atual IPV4 em atribuir um endereço IP a um determinado dispositivo:

> Esse problema decorre, na verdade, da escassez na quantidade de IPs disponíveis em sua versão 4, o qual seria solucionado com a adoção da versão 6, o chamado IPv6.

No entanto, a proposta do relatório aparentemente não considerou que o sistema IPv6 conta, por padrão, com "**extensões de privacidade**" (*privacy extensions)*, presentes em quase todos os sistemas operacionais, que **geram continuamente endereços IP efêmeros e impedem o provedor de associá-los ao titular da conexão à Internet**.

São esses os três motivos principais que nos fazem recomendar que seja removida do relatório a indicação proposta quanto ao IPV6.

14.10 Proposta nº 9: Não endossar a ampliação da guarda de registros de conexão

(Parte III - Proposições e Recomendações > 5 - Recomendações e Encaminhamentos da Comissão > b) Guarda dos registros de conexão por todos os provedores de Internet)

NOSSA PROPOSTA

Remover a promoção do PL 3237/15, que amplia o conceito de "administrador de sistema autônomo" para *aumentar* o alcance da retenção de registros de conexão à Internet.

O PL é promovido nos seguintes trechos:

- Item 2.4.2 – "Guarda dos registros de conexão por todos os provedores de internet e migração para o IPv6 ou tecnologia similar" da sub-relatoria de Segurança Cibernética no Brasil, do deputado Rodrigo Martins. (pág 137);
- Item b) na seção "3 – Proposições Legislativas em Tramitação na Câmara cuja discussão se mostra importante";
- Item nº 13 das Conclusões do Relator, deputado Espiridião Amin (pág 163).
- Sub-item ii) do item nº 22 das Conclusões do Relator, deputado Espiridião Amin (pág 168).
- Item b) da seção "5 – Recomendações e Encaminhamentos da Comissão"

Sugerimos remover, da lista de projetos de lei cujo debate têm reconhecida importância, a menção ao PL nº 3237/15, cuja finalidade é *aumentar* o alcance da retenção de dados. A proposta desse projeto de lei viola direitos fundamentais como a privacidade e a liberdade de expressão, conforme diversas pessoas da academia e da sociedade civil que se manifestaram presencialmente nesta CPI, além da Corte Interamericana de Direitos Humanos, da Corte de Justiça Europeia e de Relatores Especiais das Nações Unidas. Não há estatísticas ou estudos que justifiquem andar nesta direção, tendo havido apenas indicações anedóticas na fala de delegados e outros representantes de setores policiais ou investigativos.

Registre-se que não foi o Marco Civil da Internet o documento responsável por definir o conceito de "*Administrador de Sistema Autônomo*" (AS). A definição mencionada no art. 5º, IV, da

Lei nº 12.965/2014 incorpora a classificação já existente e reconhecida internacionalmente por meio dos *Request for Comments* (ou "pedido de comentários"), documentos técnicos desenvolvidos pela *Internet Engineering Task Force*, instituição que especifica os padrões técnicos a serem implementados e utilizados em toda a internet. O Marco Civil apenas incluiu no ordenamento jurídico brasileiro um conceito técnico já concebido e aplicado na prática, espelhando a maneira como a internet se estrutura e organiza sua dinâmica.

Assim, propor a alteração desse conceito para incluir qualquer provedor de conexão à Internet, desde que preste serviço ao público em geral, constitui uma imprecisão sem paralelo nos padrões técnicos aplicados à rede.

Além disso, o problema do referido projeto de lei não é só técnico, mas substantivo.

Primeiro, obrigar todo provedor de conexão a guardar todos os registros de conexão durante um ano implica grande custo de armazenamento seguro desses dados. Centros comunitários de acesso e outras iniciativas semelhantes, muito relevantes para a concretização dos princípios previstos no Marco Civil, seriam prejudicadas e até descontinuadas.

Em segundo lugar, a retenção de dados não é bema ceita no âmbito internacional. Conforme uma tabela feita pela empresa australiana PureVPN, referente a outubro de 2015, apenas 17 países, entre União Europeia e EUA, têm alguma lei que obrigue a guarda de registros de conexão, e 8 deles estão sob questionamento por recurso, revisão ou ação judicial. Alguns países europeus ainda estão tendo que retirar as previsões de seus ordenamentos jurídicos, desde que a retenção de dados foi julgada inconstitucional pela Corte de Justiça Europeia em 2014, por violação do direito fundamental à privacidade.

Na América Latina, a retenção de dados também é polêmica. Em todos os países onde foi proposta ou adotada, a medida encontrou forte repúdio da sociedade civil e de internautas: no Paraguai, houve a campanha contra a #Pyrawebs; no Peru, a #LeyStalker. Aqui no Brasil a obrigação da guarda de registros do Marco Civil da Internet também foi criticada, sendo "um dos pontos mais polêmicos desta discussão", como documentado no site da primeira consulta pública do MCI.

O Conselho de Direitos Humanos das Nações Unidas publicou o relatório "The Right to Privacy in the Digital Age" ("privacidade na era digital") no qual afirma que a retenção de dados interfere na privacidade até mesmo quando os dados nunca são usados – no caso, referindo-se aos programas de vigilância em massa da agência de segurança nacional dos EUA, a NSA (tradução nossa):

> Segue disso que qualquer captura de dados de comunicação é potencialmente uma interferência na privacidade e, além disso, que a coleta e retenção de dados de comunicações significa uma interferência com a privacidade quer ou não estes dados sejam posteriormente consultados ou usados. Mesmo a mera possibilidade das informações de comunicação serem capturadas cria uma interferência com a privacidade, com um efeito desencorajador (*chilling effect*) em direitos, incluindo aqueles à liberdade de expressão e associação. A própria existência de um programa de vigilância em massa então cria uma interferência com a privacidade.

Por fim, vale explicitar que todo endereço IP está ligado a um administrador de sistema autônomo, mesmo que não haja uma relação prestador-cliente entre o AS e o usuário final. Diante de um pedido ao AS, com a devida ordem judicial, será possível identificar a rede ou mesmo a máquina/dispositivo em que o IP suspeito foi utilizado, dando elementos importantes para a

continuidade das investigações (na grande maioria dos casos será possível, por exemplo, saber quando e em que local o IP foi utilizado). É assim que "crimes offline" são normalmente investigados. Não é porque a Internet tecnicamente nos permite controlar de perto a vida e as condutas de cada um, o que poderíamos fazer também no mundo offline se implantássemos chips em todos os cidadãos, que lançaremos mão de medidas que afrontam diretamente o direito à privacidade e à liberdade de expressão.

14.11 Considerações finais

Seguimos à disposição para quaisquer futuras eventualidades no encerramento dos trabalhos desta Comissão, bem no debate de propostas normativas relacionadas.

Brasília, 22 de abril de 2016.

Lucas Teixeira, diretor técnico e Joana Varon, diretora geral
Coding Rights
joana@codingrights.org (21) 98689-1313
lucas@codingrights.org (21) 99968-5003

Paulo Rená, chefe executivo de pesquisa
Instituto Beta: Internet e Democracia
paulo@ibidem.org.br (61) 8334-3055

Veridiana Alimonti, Jonas Valente e Bia Barbosa
Intervozes - Coletivo Brasil de Comunicação Social
bia@intervozes.org.br (61) 9951-4846

[RAND-VULNS-2014] ABLON, Lillian, LIBICKI, Martin C., GOLAY, Andrea A.. Markets for Cybercrime Tools and Stolen Data. National Security Research Division, RAND Corporation, EUA, 23 março 2014. Acessível em: <http://juni.pr/mhblg>. Acesso em: 22 jan. 2016.

[INFOWESTER-2009] ALECRIM, Emerson. Entendendo a Certificação Digital. InfoWester, 30 de abril de 2009. Acessível em: <http://www.infowester.com/assincertdigital.php>. Acesso em: 22 jan. 2016.

[INTERNETLAB-2016] ANTONIALLI, Dennys, ABREU, Jacqueline de Souza. Vigilância das Comunicações pelo Estado Brasileiro e a Proteção a Direitos Fundamentais. InternetLab, São Paulo, 2016.

[ARTIGO19-MCI-2015] ARTIGO 19. Marco Civil da Internet: seis meses depois, em que pé que estamos?. ARTIGO 19, 22 janeiro 2015. Disponível em: <http://artigo19.org/wp-content/uploads/2015/01/an%C3%A1lise-marco-civil-final.pdf>. Acesso em: 15 jan. 2016.

[ARTIGO19-CIBERSEG-2016] ARTIGO 19. Da Cibersegurança à Ciberguerra o Desenvolvimento de Políticas de Vigilância no Brasil. ARTIGO 19, março 2016. Disponível em: <http://artigo19.org/wp-content/blogs.dir/24/files/2016/03/Da-Ciberseguranc%CC%A7a-a%CC%80-Ciberguerra-WEB.pdf>. Acesso em: 15 jan. 2016.

[ZDNET-VULNS-2014] BLUE, Violet. Hackonomics: Street prices for black market bugs. ZDNet, CBS, EUA, 16 abril 2014. Disponível em: <http://www.zdnet.com/article/hackonomics-stolen-twitter-accounts-more-valuable-than-credit-cards/>. Acesso em: 22 jan. 2016.

[WIRED-SR2-2015] BRANDOM, Russel. Feds found Silk Road 2 servers after a six-month attack on Tor. The Verge, 21 janeiro 2015. Disponível em: <http://www.theverge.com/2015/1/21/7867471/fbi-found-silk-road-2-tor-anonymity-hack>. Acesso em: 22 jan. 2016.

[BRASIL-VERDE-2010] BRASIL, Presidência da República. Livro Verde: Segurança Cibernética no Brasil. Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações, 2010. Disponível em: <http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_ Acesso em: 22 jan. 2016.

[BRASIL-CIBERSEG-2015] BRASIL, Presidência da República. Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal. Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações, março 2015. Disponível em: <http://dsic.planalto.gov.br/documentos/publicacoes/4_Estrat Acesso em: 22 jan. 2016.

[BRASIL-DARKNET-2014] BRASIL, Portal. Polícia Federal identifica 90 pessoas que compartilham pornografia infantil. Portal Brasil, 15 outubro 2014. Disponível em: <http://www.brasil.gov.br/defesa-e-seguranca/2014/10/policia-federal-identifica-90-pessoas-que-compartilham-pornografia-infantil>. Acesso em: 22 jan. 2016.

[CONJUR-2016] CANÁRIO, Pedro. Sigilo de fonte é essencial para direito de informar, afirma Celso de Mello. Revista Consultor Jurídico, Brasília, 5 outubro 2015. Disponível em: <http://www.conjur.com.br/2015-out-05/sigilo-fonte-essencial-informar-afirma-celso-mello>. Acesso em: 15 jan. 2016.

[CAPANEMA-2012] CAPANEMA, Walter. O Direito ao Anonimato. 2012. Disponivel em:

<http://www.avozdocidadao.com.br/images_02/artigo_walter
Acesso: 22 jan. 2016.

[GUARDIAN-WILDLEAKS-2014] CARRINGTON, Damian. WildLeaks attracts major wildlife crime leads in first three months. The Guardian, 12 junho 2014. Disponível em: http://www.theguardian.com/environment/2014/jun/12/wildle illegal-wildlife-crime>. Acesso em: 22 jan. 2016.

[CIDH-2009] CORTE INTERAMERICANA DE DIREITOS HUMANOS. Caso Escher e outros vs. Brasil. Sentença de 6 julho 2009, Parágrafo 114. Disponível em <http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_p
Acesso em: 17 jun 2015

[COSATE-2009] COSATE, Tatiana Moraes. Liberdade de informação e sigilo da fonte. Revista Jus Navigandi, Teresina, ano 14, n. 2152, 23 maio 2009. Disponível em: <https://jus.com.br/artigos/12767>. Acesso em: 15 jan. 2016.

[DISQUEDENUNCIA] Disque-Denúncia. Website Disque Denúncia, Rio de Janeiro. Disponível em: <http://disquedenuncia.org.br/o-disque-denuncia>. Acesso em: 15 jan. 2016.

[FSF-Jpp-GNUPG-2014] FOUNDATION, Free Software, JORNALISM++. Autodefesa no E-mail. Free Software Foundation, junho 2014. Disponível em: <https://emailselfdefense.fsf.org/pt-br/>. Acesso em: 22 jan. 2016.

[EC-CIBERSEG-2013] EUROPEAN COMISSION. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. High Representative of the European Union for Foreign Affairs and Security Policy, Bruxelas, 7 fevereiro 2013. Disponível em: <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=16
Acesso em: 22 jan. 2016.

[FOCWG1-CIBERSEG-2015] FREEDOM ONLINE COALITION. Recommendations for Human Rights Based Approaches to Cybersecurity, Discussion draft. Freedom Online Coalition Working Group 1 (“An Internet Free and Secure”), 21 setembro 2015. Disponível em:

<https://www.freedomonlinecoalition.com/wp-content/uploads/2015/11/FOC-WG1-Recommendations-discussion-draft-IGF-2015-new.pdf>. Acesso: 22 jan. 2016.

[OLHARDIGITAL-TORCMU-2015] GONÇALVES, Jefferson. Serviço Tor acusa universidade de aceitar dinheiro do FBI para espionagem. Fique Seguro, Olhar Digital, 19 novembro 2015. Disponível em: <http://olhardigital.uol.com.br/fique_seguro/noticia/servico-tor-acusou-universidade-de-aceitar-dinheiro-do-fbi-para-espionagem/53123>. Acesso em: 22 jan. 2016.

[VICE-DARKNET-2014] JORDAN, Lucy. Brazilian Police Bust 'Darknet' Child Pornography Ring. VICE News, 16 outubro 2014. Disponível em: <https://news.vice.com/article/brazilian-police-bust-darknet-child-pornography-ring>. Acesso em: 22 jan. 2016.

[KAYE-2015] KAYE, David. Report on encryption, anonymity, and the human rights framework. Nações Unidas, Conselho de Direitos Humanos, 2015. Disponível em: <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/ Acesso em: 22 jan. 2016.

[KNOTT-WROE-2015] KNOTT, Matthew, WROE, David. Abbott government's metadata plan tipped to cost $300m. The Sydney Morning Herald, Sydney, 19 fevereiro 2015. Disponível em: <http://www.smh.com.au/federal-politics/political-news/abbott-governments-metadata-plan-tipped-to-cost-300m-20150218-13iii7.html>. Acesso em: 22 jan. 2016.

[MENDES-PINHEIRO-2015] MENDES, Gilmar Ferreira, PINHEIRO, Jurandi Borges. Interceptações e Privacidade: novas tecnologias e a Constituição. Direito, Inovação e Tecnologia, Volume 1, 2015. Página 231.

[MENDES-2015] MENDES, Laura Schertel. Uso de softwares espiões pela polícia: prática legal?. JOTA, 4 junho 2015. Disponível em: <http://jota.info/uso-de-softwares-espioes-pela-policia-pratica-legal>. Acesso em: 22 jan. 2016.

[G1-2007] MENDONÇA, Alba Valéria. Solução de crimes depende de ajuda da população. G1, Rio de Janeiro, 10 março 2007. Disponível em: <http://g1.globo.com/Noticias/Rio/0,,MUL9408-5606,00-SOLUCAO+DE+CRIMES+DEPENDE+DE+AJUD Acesso em: 15 jan. 2016.

[NATGEOBR-WILDLEAKS-2014] MENDONÇA, José Eduardo. WildLeaks, a plataforma contra a caça ilegal e o tráfico de animais selvagens. Planeta Urgente - Planeta Sustentável, National Geographic Brasil, 29 agosto 2014. Disponível em: <http://viajeaqui.abril.com.br/materias/wildleaks-plataforma-contra-caca-ilegal-trafico-de-animais-selvagens>. Acesso em: 22 jan. 2016.

[OECD-ENGAGEMENT-2015] OECD. Council Resolution on Enlargement and Enhanced Engagement - Organisation for Economic Co-operation and Development, maio 2013. Disponível em: <http://www.oecd.org/brazil/oecdcouncilresolutiononenlarger Acesso em: 22 jan 2016.

[OECD-SEOUL-2008] OECD. Civil Society Seoul Declaration. OECD Ministerial conference on the Future of the Internet Economy, Seoul, 16 junho 2008. Disponível em: <http://csisac.org/seoul.php>. Acesso em: 22 jan 2016.

[OEAeBID-CIBERSEGLATAM-2016] Cybersecurity: Are We Ready in Latin America and the Caribbean?. OEA e Banco Nacional Interamericano, 15 março 2016. Disponível em: <https://publications.iadb.org/bitstream/handle/11319/7449/C Are-We-Prepared-in-Latin-America-and-the-Caribbean.pdf?sequence=1>. Acesso em: 15 jan 2016.

[OECD-RISK-2015] OECD. Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris, 2015. Disponível em: <http://dx.doi.org/10.1787/9789264245471-en>. Acesso: 22 jan. 2016

[PAULO-ALEXANDRINO-2007] PAULO, Vicente; ALEXANDRINO, Marcelo. Direito Constitucional Descomplicado. 1a, 3a tiragem. Niterói: Impetus, 2007. p.118.

[UN-PRIVACY-2014] PILLAY, Navi. The Right to Privacy in the Digital Age. Nações Unidas, Conselho de Direitos Humanos, 2015. Disponível em: <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/ Acesso em: 22 jan. 2016.

[UNGA-CRIMINAL-2001] UNITED NATIONS GENERAL ASSEMBLY. Resolution adopted by the General Assembly on the report of the Third Committee (A/55/593) - Combating the criminal misuse of information technologies. 22 jan 2001. Disponível em: <https://www.unodc.org/documents/commissions/CCPCJ/Cri 2009/2000/General_Assembly/A-RES-55-63.pdf>. Acesso em: 22 jan. 2016.

[13-PRINCIPIOS] Princípios Internacionais sobre a Aplicação Dos Direitos Humanos na Vigilância Das Comunicações. Necessary and Proportionate, maio 2014. Disponível em: <https://pt.necessaryandproportionate.org/text>. Acesso em: 22 jan. 2016.

[PUDDEPHATT-KASPAR-CIBERSEG-2015] PUDDEPHATT, Andrew, KASPAR, Lea. Cybersecurity is the new battleground for human rights. openDemocracy, 18 novembro 2015. Disponível em: <https://www.opendemocracy.net/wfd/andrew-puddephatt-lea-kaspar/cybersecurity-is-new-battleground-for-human-rights>. Acesso em: 22 jan. 2016.

[MELLO-STF-1996] Relator: Ministro Celso de Mello INQ – 870 /RJ. Data de julgamento 08/04/1996. Data de Publicação: DJ 15/04/1996 Disponível em: <http://stf.jusbrasil.com.br/jurisprudencia/14758836/inquerito inq-870-rj-stf>. Acesso em: 15 jan. 2016.

[ROSSINI-CIBERSEG-2015] ROSSINI, Carolina. Ciberseguridad e el rol de la Sociedad Civil. Public Knowledge, Buenos Aires, junho 2015. Disponível em: <http://pt.slideshare.net/carolina.rossini/ciberseguridad-y-el-rol-de-la-sociedad-civil>. Acesso em: 15 jan. 2016.

[ROSSINI-OEA-2015] ROSSINI, Carolina. Segurança cibernética na Latino América: atuação da OEA. Boletim Antivigilância, Coding Rights, 17 junho 2015. Disponível em: <https://antivigilancia.org/pt/2015/06/construa-sua-seguranca-a-atuacao-da-oea-na-

seguranca-cibernetica/>>. Acesso em: 15 jan. 2016.

[SARAVA-2014] SARAVÁ, Coletivo. Marco Civil: abacaxi não é alicate. Saravá.org, 28 maio 2014. Disponível em: <https://www.sarava.org/pt-br/content/marco-civil-abacaxi-n%C3%A3o-%C3%A9-alicate>. Acesso em: 27 jan. 2016.

[SOLOVE-PRIVACY-2008] SOLOVE, Daniel J., I've Got Nothing to Hide" and Other Misunderstandings of Privacy. 12 julho 2007. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565> Acesso em: 22 jan. 2016.

[SWEENEY-2000] SWEENEY, Latanya. Simple Demographics Often Identify People Uniquely. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh, 2000. Acessível em: http://dataprivacylab.org/projects/identifiability/paper1.pdf>. Acesso em: 22 jan. 2016.

[SYVERSON-2011] SYVERSON, Paul F. A Peel of Onion. Twenty-Seventh Annual Computer Security Applications Conference, dezembro 2011. Disponível em: <https://www.acsac.org/2011/program/keynotes/syverson.pdf Acesso em: 15 fev. 2016.

[ANTIVIG-MCI-2-2014] VARON, Joana e CASTANHEIRA, Bruna. Marco Civil é aprovado durante o NetMundial, mas ainda precisa ser regulado: o que esses dois marcos históricos nos dizem sobre a proteção da privacidade no Brasil? Boletim Antivigilância, 3 junho 2014. Disponível em: <https://antivigilancia.org/pt/2014/06/marco-civil-e-aprovado-durante-o-netmundial-mas-ainda-precisa-ser-regulado-o-que-esses-dois-marcos-historicos-nos-dizem-sobre-a-protecao-da-privacidade-no-brasil/>. Acesso em: 15 fev. 2016.

[ANTIVIG-CHATANONIMO-2015] TEIXEIRA, Lucas. Tor Messenger e Ricochet: chat anônimo no computador. Boletim Antivigilância, Coding Rights, 9 novembro 2015. Disponível em: <https://antivigilancia.org/pt/2015/11/trackers-os-grandes-stalkers-da-web/>. Acesso em: 22 jan. 2016.

[ANTIVIG-TRACKERS-2015] TEIXEIRA, Lucas. Trackers: os grandes stalkers da Web Boletim Antivigilância, Coding Rights, 9 novembro 2015. Disponível em: <https://antivigilancia.org/pt/2015/11/tor-messenger-e-ricochet-chat-anonimo/>. Acesso em: 22 jan. 2016.

[THOUGHTWORKS-2014] THOUGHTWORKS. Technology Radar da ThoughtWorks identifica perigosa tendência em armazenamento de dados Big Data. ThoughtWorks, São Paulo, 13 fevereiro 2014. Disponível em: <https://mingle.thoughtworks-studios.com/cn/news/technology-radar-jan-2014-brasil>. Acesso em: 22 jan. 2016.

[TICDOMICILIOS-2015] TIC DOMICÍLIOS. Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nos domicílios brasileiros - TIC Domicílios 2014. NIC.br / Cetic.br, 23 de novembro de 2015. Disponível em: <http://www.cetic.br/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-domicilios-brasileiros/>. Acesso em: 22 jan. 2016.

[ITU-CIBERSEG-2008] INTERNATIONAL COMMUNICATIONS UNION. Series X: Data Networks, Open System Communications and Security - Telecommunication Security - Overview of cybersecurity (Recommendation ITU-T X.1205). Telecommunication Standardization Sector of ITU (ITU-T), Genebra, abril 2008.Disponível em: <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=en>. Acesso em: 22 jan. 2016.

[ITU-GCA] INTERNATIONAL COMMUNICATIONS UNION. Global Cybersecurity Agenda (GCA). Disponível em: <http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx>. Acesso em: 22 jan. 2016.

[ANTIVIG-24EC-2014] VARON, Joana e CASTANHEIRA, Bruna. Corte de Justiça da União Européia invalida Diretiva de Retenção de Dados. Boletim Antivigilância, Oficina Antivigilância, 3 junho 2014. Disponível em: <https://antivigilancia.org/pt/2014/06/corte-de-justica-da-uniao-europeia-invalida-

diretiva-de-retencao-de-dados/>. Acesso em: 15 jan. 2016.

[JOANA-ONU-2015] VARON, Joana. Anonimato e eleição do relator especial de privacidade trazem políticas de Internet para o Conselho de Direitos Humanos da ONU. Boletim Antivigilância, Coding Rights, 10 julho 2015. Disponível em: <https://antivigilancia.org/pt/2015/07/anonimato-e-eleicao-do-relator-de-privacidade-sao-destaque-nas-reuniao-do-conselho-de-direitos-humanos/>. Acesso em: 22 jan. 2016.

[ANTIVIG-MCI-2014] VARON, Joana. Artigo 16º da nova versão do Marco Civil enfraquece a proteção à privacidade dos usuários. Boletim Antivigilância #6, Oficina Antivigilância, 13 de dezembro de 2013. Disponível em: <https://antivigilancia.org/pt/2013/12/artigo-16o-da-nova-versao-do-marco-civil-enfraquece-a-protecao-a-privacidade-dos-usuarios/>. Acesso em: 15 jan. 2016.

[VICKY-JEFFERSON-2007] VICKY, Vovó. Cilindro de Jefferson. Aldeia Numaboa, 3 julho 2007. Disponível em: <http://numaboa.com.br/criptografia/substituicoes/polialfabet jefferson>. Acesso em: 15 jan. 2016.

[WALLACE-ANON-1999] WALLACE, Kathleen A. Anonymity. Department of Philosophy, Hofstra University, NY, USA, 1999.

[WALLACE-ANON-2008] WALLACE, Kathleen A. Online Anonymity. The Handbook of Information and Computer Ethics, New Jersey, EUA, 2008. Disponível em: <http://www.cems.uwe.ac.uk/~pchatter/2011/pepi/The_Handl Acesso em: 15 jan. 2016.

[WRIGHT-TOR-2015] WRIGHT, Jordan. How Tor Works. jordan-wright, 28 fevereiro 2015. Acessível em: <http://jordan-wright.com/blog/2015/02/28/how-tor-works-part-one/>. Acesso em: 22 jan. 2016.