Universidade de Brasília

Instituto de Ciências Exatas

Departamento de Ciência da Computação

Privacidade na rede aberta

Piotr Pisarewicz

Monografia apresentada como requisito parcial
para conclusão do Curso de Computação – Licenciatura

Orientador:
prof. Pedro Antônio Dourado de Rezende

Brasília
2013

Universidade de Brasília UnB
Instituto de Ciências Exatas
Departamento de Ciência da Computação
Curso de Computação Licenciatura

Coordenador: Prof. Dr. Coordenador

Banca examinadora composta por:

Prof. Pedro Antônio Dourado de Rezende (Orientador) – CIC/UnB
Prof. Dra. Maria de Fátima Ramos Brandão – CIC/UnB
Prof. Dr. Jorge Henrique Cabral Fernandes – CIC/UnB

CIP — Catalogação Internacional na Publicação

Piotr Pisarewicz
Privacidade na rede aberta / Piotr Pisarewicz. Brasília : UnB, 2013. 86 p. : il. 3; 29,5 cm.

Monografia (Graduação) Universidade de Brasília. Brasília, 2013.

1. privacidade, 2. internet.

CDU 004.4

Endereço: Universidade de Brasília
Campus Universitário Darcy Ribeiro # Asa Norte
CEP 70910-900
Brasília–DF — Brasil

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Privacidade na rede aberta

Piotr Pisarewicz

Monografia apresentada como requisito parcial
para conclusão do Curso de Computação – Licenciatura

Prof. Pedro Antônio Dourado de Rezende (Orientador)
CIC/UnB

Prof. Dra. Maria de Fátima Ramos Brandão
CIC/UnB

Prof. Dr. Jorge Henrique Cabral Fernandes
CIC/UnB

Prof. Dr. Coordenador
Flávio de Barros Vidal
CIC/UnB

Brasília, 23 de julho de 2013

Dedicatória

Dedico a persente monografia à minha mãe.

Agradecimentos

Agradeço ao Sr. Prof. Pedro Antônio Dourado de Rezende que depois de ter ampliado os meus horizontes de pensamento concordou em enfrentar os efeitos disso e ser orientador da presente monografia.

Resumo

O autor apresenta sua percepção da privacidade na época digital com o foco particular na interação dos usuários com a rede aberta. A privacidade é cogitada como a soberania de indivíduos em definir e desempenhar de forma autônoma seus papeis sociais, com ênfase em elementos de caráter instintivo na privacidade. A monografia analisa o uso comum da rede aberta, frisando vantagens, mas também indicando as ameaças à privacidade e até à cidadania e liberdade. O autor enumera e avalia as tecnologias e agentes invasores e indica os possíveis métodos de defesa, partindo da suposição que a proteção da privacidade é um dos aspectos primordiais em sociedades pós-modernas democráticas, sadias e prósperas. O autor tende a provar que a erosão multilateral da privacidade, observada globalmente, abre caminhos para distorções dos sistemas comumente percebidos como democráticos, ameaça a liberdade e cria fundamentos para surgimento de novos tipos de totalitarismos.

Palavras-chave: privacidade, internet

Sumário

Lista de Figuras

Lista de Tabelas

Introdução

A internet, hoje em dia, é chamada de "rede global". O adjetivo "global" pode descrever tanto seu alcance técnico quanto sua capacidade de transpassar as fronteiras estaduais e unir pessoas de todas as culturas, o que corresponde à globalização onipresente. Porém, quanto ao alcance, a internet ainda não merece esse adjetivo, já que menos de um terço da população mundial tem acesso a ela. Ela apenas tende a ser global, o que, talvez, denomine o seu futuro limite de alcance. O termo "rede aberta" é o que verdadeiramente reflete a sua natureza, tanto física quanto social. Mesmo assim, nesta monografia, o termo "rede global", aparentemente um pouco exagerado, é considerado como equivalente ao termo "rede aberta" e à internet. Uma outra inadequação vem do fato de a internet ser comumente confundida com o serviço WWW, principalmente por causa da mídia tradicional, que o trata de maneira particular, como algo que a ameaça do ponto de vista comercial e, por isso, fica superestimado como um centro de peso da rede global como um todo.

Contudo, a internet é a maior rede mundial de informação e seu crescimento não para. Ela foi concebida por motivos bélicos no mundo militar. Fornecendo resiliência e rapidez de troca de dados, tornou-se atraente também para o meio acadêmico, onde essa qualidade é de suma importância. Hoje, tal rede é realmente aberta e pode ser acessada pelas pessoas comuns. Logo depois do surgimento da WWW, a internet começou a virar-se para sua utilidade comercial e isso é hoje sua caraterística predominante[1]. Muitas empresas perceberam o seu potencial como plataforma de comunicação com clientes e outras entidades, meio de propaganda, espaço para construir lojas virtuais, efetuar transações, entre outras funções. A internet oferece um acervo gigantesco de serviços: comercias, financeiros, de educação, de entretenimento, entre outros. Ela inscreveu-se no quadro social e continua influenciando praticamente todos os domínios da vida das pessoas, pelo menos nas economias mais desenvolvidas. Criou novos tipos de profissões, novos modelos de negócio e gerou novas palavras em vários idiomas do mundo (anglicismos, via de regra) e novos padrões de comportamento.

Mas a rede aberta não é um "bem absoluto", como qualquer outra invenção significativa conhecida na história da humanidade. As novas tecnologias sempre geraram grande otimismo na sua fase inicial e as vozes capazes de indicar as possíveis desvantagens eram raras e soavam baixo, distantes em meio ao entusiasmo geral. Não é surpresa que a rede aberta também siga esse padrão. Ela tem suas facetas sombrias. O otimismo que a acompanha baseia-se não só em promessas de vantagens, mas, antes de tudo, na ignorância dos usuários no que diz respeito às tecnologias e aos riscos associados a elas, inércia dos sistemas legislativos, da natureza "quase-caótica" dos sistemas informacionais embutidos na rede aberta e da nossa natureza humana, gananciosa, nervosa, impaciente e viciada em mitos. A lista de *drawbacks* da rede aberta cresce praticamente sem fim, como comprovam os noticiários diários.

A internet passou a infância dando a impressão de ser uma jovem promissora, sendo comparada à noosfera de Vernadsky e à aldeia global de McLuhan. Teve chances de ser uma entidade democrática, aberta e livre. Muitos a associam com rapidez, riqueza de recursos, opções e, também, com anonimato. Essa última vantagem vem a ser altamente discutível. A internet, como a presente monografia propõe demonstrar, não oferece nenhum anonimato absoluto, porém, com um certo conhecimento tecnológico avançado é possível ficar anônimo o bastante. Essa sua caraterística resultou em uma avalancha crescente de cibercrimes. A luta contra eles é muito difícil, e os perpetradores, via de regra, acabam impunes. A maioria dos crimes na internet é ligada a violações de privacidade, embora a definição desta seja nebulosa. O anonimato de usuários leigos tornou-se mais um mito da época digital, pois muitas entidades estatais e comerciais desejam e conseguem monitorar seus usuários. Surgiram

1 Fala-se da sua parte visível através de motores de busca. A parte invisível, a Deep Web, é muito maior.

vários métodos de efetuar esse monitoramento, e ele tornou-se onipresente. Na fase atual do seu desenvolvimento, a internet parece ser realmente impregnada de vigilância, o que ameaça não só a privacidade, mas, até mesmo, a liberdade de pessoas. Marcella e Stucki em *Privacy Handbook* colocam o seguinte subtítulo na Introdução da sua obra: *Privacidade na época da vigilância (Privacy in an Age of Vigilance)*[2]. Não é mesmo que hoje o adjetivo "digital" se relaciona e até em certas situações se confunde com "vigiado"?

Temos, também, cada vez mais exemplos de como a rede aberta pode ser utilizada para confrontar os sistemas políticos percebidos, em certos contextos, como perversos, mas não só eles. *Wikileaks*, Primavera Árabe de 2010-2011, eleições parlamentares na Rússia em 2011, guerra civil na Síria (continua desde março de 2011), protestos em massa no Brasil em 2013 e outros, são exemplos que confirmam esse potencial político. Conscientizar e unir as pessoas para enfrentar os perigos sociopolíticos e de outros tipos nunca foi tão fácil quanto na época digital, e é óbvio – e de se esperar – que as esferas políticas déspotas, mas também as comumente percebidas como democráticas, reajam com grande nervosismo perante essas percebíveis ameaças. Um exemplo relevante constitui o "separatismo informacional" da China. Mas as ameaças oriundas da rede aberta são muitas, e de naturezas diferentes. Não só os déspotas devem temê-las hoje em dia. A capacidade da rede de unir as pessoas significa, também, a capacidade de verificar quem teve a ousadia de se unir.

Não surpreendentemente, parece-nos que a rede criada por humanos ficou semelhante ao próprio humano, com suas forças e fraquezas, virtudes e pecados. Será que ela perdeu a chance de melhorar (por si mesma)? Evidentemente, seus pecados aumentam tão rápido quanto seu alcance técnico. A opinião sobre a sua relevância e necessidade incontornável parece-nos ser tão exagerada quanto a de se possuir aparelho de televisão ou de rádio, uma vez que cogitamos conceitos tão primordiais como o da proteção da condição humana; em particular, o da proteção de privacidade.

Contudo, a rede aberta continua sendo útil para os usuários, mas a preço de eles serem vigiados, grampeados, cobiçados como alvo de propaganda, perseguidos como possíveis infratores da propriedade intelectual, caçados por novos tipos de criminosos e controlados por autoridades, empregadores ou até seus próximos ou por qualquer outra pessoa ou entidade. Geralmente, os usuários não estão cientes dessas ameaças ou as desprezam; e, em geral, não reagem. Alguns até percebem que "algo ruim" está acontecendo, mas não são capazes de encontrar o contexto mais abstrato em que isso faz sentido, não percebem as mudanças sociais de longo prazo. Eles utilizam a rede aberta com uma ingenuidade alarmante, navegam nela como descobridores de uma vantagem prodigiosa e inquestionável.

Como resultado disso, sua privacidade torna-se uma mercadoria, que eles entregam a troco de nada, literalmente se subordinando aos demandantes desse novo bem, que surgem em profusão. A questão de tratamento da privacidade como um bem a ser comercializado, versus um direito humano fundamental a ser protegido, é particularmente visível quando confrontamos as culturas e os sistemas legais dos Estados Unidos e da União Europeia. Nos Estados Unidos, o novo mercado de dados e novos tipos de negócios na internet são percebidos mais como uma grande fronteira de oportunidades, enquanto que em países da União Europeia prevalece um posicionamento mais reservado, no qual as desvantagens da primeira abordagem (mercantil), já existentes ou possíveis, ficam no foco das discussões legais e sociais sobre a proteção da condição humana.

Entre provedores de serviços na rede, negociantes de dados e autoridades controladoras, os interesses que governam esse meio de comunicação relativamente novo ficam óbvios: proteção de interesses econômicos e políticos, isto é, da mesma natureza das relações político-econômicas nas sociedades contemporâneas. O caminho para atingir esses

2 Albert J. Marcella, Jr., Carol Stucki, "Privacy Handbook, Guidelines, Exposures, Policy Implementation, and International Issues".

objetivos é identificar os usuários da rede e conhecer tudo o que seja possível sobre eles, coletando, agregando e analisando os dados, em particular os pessoais, observando padrões de navegação, analisando e-mails, históricos de compras em lojas virtuais, dados "em nuvem", e construindo seus perfis ou identidades digitais. A internet é o único meio semiológico na História que permite fazer a identificação e o "grampo" de interlocutores em volume, organização e tempo potencialmente ilimitados. Esse aspecto, que ameaça a privacidade dos usuários da rede aberta, é tema de miliares de monografias, dissertações e livros, e não pára de ser o foco de várias discussões atuais.

Cabe ressaltar que qualquer obra sobre a privacidade na rede aberta, particularmente no que se refere à questão tecnológica, desatualiza-se instantaneamente, pois as invenções técnicas que ameaçam a privacidade ou que tendem a protegê-la aparecem quase diariamente. Essa situação é parecida com a do *doping* na esfera do esporte profissional, que lida com problemas da detecção e camuflagem de bioquímica ilícita. Após cada substância legalmente proibida, aparecem várias novas, mais modernas, mais difíceis de detectar, de compreender seu funcionamento e de combater. O desenvolvimento vertiginoso da tecnologia moderna, e as vantagens e os problemas que a acompanham no que diz respeito à privacidade, parecem formar uma "Tempestade Perfeita"[3], Como será o futuro da privacidade, permanece uma questão candente. De acordo com os autores da analogia, Craig e Ludolf, esse futuro é agora.

1. Rede aberta contemporânea

1.1. Uso cotidiano dos serviços na rede aberta

Conforme a Internet Usage Statistics[4], em junho de 2013 a internet apresentava mais de 2,4 bilhões de usuários. Isso constitui aproximadamente 34% da população mundial, que somava cerca de 7 bilhões em 2012. O número de internautas em 2013 cresceu quase 6 vezes em comparação com o ano 2000. A maior penetração por regiões se dá na América do Norte, onde 78,6% da população utilizando a internet, seguida pela Austrália e Oceania, com 67,6%, e da Europa, com 63,2%. A América Latina e Caribe têm quase 255 milhões de usuários, o que constitui 42,9% da população. A taxa de crescimento nessa região aumentou em mais de 1300% durante o período de 2000-2013. O crescimento da popularidade da internet é impressionante. Ela influenciou numerosas esferas da nossa vida, e continua adentrando nelas. A mídia tradicional, como rádio, televisão, imprensa, telefone, correio, música e filme existem paralelamente no espaço virtual da internet e surgem receios de que o seu futuro fora dela esteja condenado.

Do ponto de vista de um usuário comum, os usos mais comuns da internet hoje em dia (omitindo-se a pornografia, fato que, na verdade, não é justificado, dado o tráfico dedicado a ela): são

- busca de informações (fonte de conhecimento, educação, etc.);
- caixa de e-mail;
- redes sociais;
- discussões (grupos, fóruns, listas de discussões e-mail, etc.);
- IRC (conversas textuais em tempo real);
- blogs;
- comunicadores de internet, por exemplo: ICQ, Jabber, Skype;
- telefonia de Internet (VoIP – Voice over IP ou Voz sobre IP)
- serviços bancários eletrônicos;
- mídia de Internet (rádio, televisão, imprensa, portais);
- compras em lojas virtuais;

3 Terence Craig e Mary E. Ludolf, "Privacy and Big Data".

4 http://www.internetworldstats.com/stats.htm (carregado em 10 de outubro de 2011).

- entretenimento (jogos online);
- leilões de Internet;
- teleconferências.

Do ponto de vista das empresas comuns, os usos mais comuns incluem:

- anunciar sobre si, seus produtos e serviços;
- vender produtos e serviços online;
- buscar informações relevantes para seu negócio;
- utilizar serviços bancários e financeiros;
- trocar informações com outras empresas e instituições (via e-mail);
- interconectar seus filiais;
- coletar dados sobre os usuários de seus serviços.

Existem empresas para as quais a internet não é só um meio de comunicação, mas também o próprio negócio (*ad serving*). Elas são descritas adiante.

Do ponto de vista das instituições não comerciais privadas e públicas, os usos mais comuns incluem:

- informar sobre si mesma, seus serviços;
- oferecer serviços online (bancos de dados, serviços para a cidadania);
- trocar informações com outras instituições (via e-mail);
- interconectar seus filiais;
- coletar dados sobre os usuários de seus serviços.

O acervo gigantesco de dados cria possibilidades para suporte à educação, embora, no caso de crianças e jovens, exista a necessidade de se acompanhar a interação deles com a rede aberta, já que eles não dispõem de, por assim dizer, maturidade informacional.

1.2. Perigos na rede aberta

A rede global, por causa da sua construção técnica e lógica, facilidade de acesso e dificuldade de controle (dependendo de quem queira efetuá-lo), ineficácia ou falta de leis, grande alcance, modelo de construção de hardware e software, e, principalmente, por causa da nossa própria natureza humana, não é segura e nunca o será. Esses problemas resultam na onipresença de cibercrimes e da abordagem mercantil à privacidade, com coleta de dados sobre usuários por governos, empresas, empregadores e outros demandantes.

A já citada ineficácia ou inexistência de lei, e a complexidade e sutileza técnica dos ataques e crimes no ciberespaço, ficam ainda mais agravados por causa da escassez de peritos e métodos eficazes de forênsica e operadores legislativos capazes de lidar, efetivamente e com isenção, com essa classe de problemas. A inércia dos sistemas legislativos, e sua natureza conservadora ou reativa, causam inadequação permanente e atraso crônico em relação aos avanços tecnológicos e às mudanças sociais causadas por eles, inclusive no que se refere às novas modalidades de crime. Por motivos difíceis de resumir, quase sempre relacionados à dificuldade de se comprovar dolo na autoria, os crimes sérios cometidos com a utilização da rede e descobertos a tempo não enfrentam reações penalizantes, adequadas ao seu papel potencialmente inibidor, por parte da justiça. Em vários casos, até parece que os sistemas jurídicos atuam conforme a opinião pública, que tende a demonstrar alguma compaixão com certos tipos de criminosos digitais. Como esse tipo de crime exige preparação técnica e inteligência invejáveis, aqueles capazes de invadir os sistemas informáticos grandes ou muito importantes parecem merecer reconhecimento público. O filme *Takedown*, sobre a história da prisão do hacker Kevin Mitnick, é um exemplo de tal apreciação.

Entre as duas abordagens, a atividade estatal parece viver uma dualidade "orweliana". Enquanto os parlamentos estabelecem as leis para proteger a privacidade, os governos e suas agências convocadas para proteger a segurança pública infiltram a rede sem o mínimo ou sem

nenhum controle efetivo por parte da sociedade.

Entre as condutas que podem ser tipificadas como crime digital, o "roubo de identidade" (furto) se torna cada vez mais comum.

A rede global criou possibilidades de se coletar dados sobre seus usuários sem consentimento nem conhecimento deles, o que gera numerosos riscos. Esses dados podem ser obtidos por interesses diversos, o que gera ameaças diretas e óbvias aos usuários, não só pelo risco de furto da identidade por parte de criminosos, mas também pelo interesse de instituições públicas, particularmente em países com regimes que violam os direitos humanos (mas não só neles). Também gera ameaças diretas, mas já não tão óbvias, pelo interesse de empresas de *marketing* que desejam saber o máximo possível sobre nós, usuários da rede, em ganhar dinheiro vendendo esses dados.

Entre as entidades comerciais, um grupo demonstra cada vez maior interesse em vigiar e controlar os usuários – os detentores de propriedade intelectual (*Intellectual Property Stakeholders*). Nesse grupo encontram-se grandes produtores de *ebooks*, áudio, vídeo, software, entre outros.

Os empregadores tendem a desconfiar da idoneidade profissional dos empregados e controlam seus e-mails, sua interação com a internet, ema particular as visitas nas redes sociais. Na pesquisa da AMA de 2007[5], dois terços de empregadores monitoram o uso da internet pelos seus empregados.

Os provedores de acesso à internet ocupam um lugar particular na comunicação pela rede aberta. Eles podem interceptar e gravar as requisições dos usuários aos servidores.

Infelizmente, podemos ficar rastreados também por nossos próximos: cônjuges, filhos, parentes, colegas e amigos.

O acesso à rede pelas crianças e adolescentes também gera preocupações. Estes não são capazes de avaliar quão perigosas podem ser certas interações suas pela rede, frente às quais um adulto, mesmo leigo, comportar-se-ia de maneira mais cautelosa. A aquisição de dados de menores de idade é muito mais fácil do que em situações gerais, envolvendo normalmente adultos. Além de perigos ligados à pornografia infantil e ao abuso de menores, as crianças enfrentam vários riscos de manipulação psicológica que, mesmo não sendo ilegais, podem ser mentalmente devastadoras[6].

Em várias áreas supramencionadas, o núcleo de ameaças se origina na coleta e processamento de *dados pessoais,* e o uso destes com objetivos frequentemente diferentes daqueles anunciados pelos provedores de serviços aos usuários. As verdadeiras intenções ficam ocultas ou camufladas tanto aos usuários quanto às entidades convocadas para controlar o uso desses dados.

A drenagem da privacidade na época digital ameaça a liberdade, pois a privacidade é um elemento essencial dela.

2. Aspetos da privacidade na rede aberta

2.1. Definição de dados pessoais

O termo Informação Pessoalmente Identificável (*Personal/Personally Identifiable Information*), comumente abreviado como PII é frequentemente tratado como conceito jurídico e, em vários sistemas da lei, ele pode compreender vários tipos de informação. Por exemplo, a diretiva base da União Europeia convoca a seguinte definição, no Artigo 2º, inciso a):

5 American Managment Association, 2007 Electronic Monitoring & Surveillance Survey, http://press.amanet.org/press-releases/177/2007-electronic-monitoring-surveillance-survey/ (carregado em 22 de junho de 2013).

6 Vários relatórios sobre casos reais de cyberbullying e sexting podem ser encontrados no Cyberbullying Research Center, http://cyberbullying.us/ (carregado em 22 de junho de 2013).

"Dados pessoais", qualquer informação relativa a uma pessoa singular identificada ou identificável ("pessoa em causa"); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social.

Cabe ressaltar que os termos "dados" e "informação" são comumente usados como sinônimos, mas existe uma diferença significativa entre eles. Dados devem ser compreendidos apenas como sequências de símbolos. A interpretação deles, pela atribuição de um certo contexto a eles, é que os leva a representar informação. Por exemplo, uma cadeia de algarismos 65022200382 por si só não significa nada, mas sabendo que ela aqui representa o número de identificação de uma pessoa (o contexto), já se pode identificar o indivíduo – portador desse número[7]. Isso seria um exemplo da identificação indireta, conforme a definição supramencionada. Os dados pessoais na definição supramencionada já são informação, pois o adjetivo "pessoal" e o resto da definição, dada ali por nomes ou rótulos dos campos no registro dos dados (metadados), criam os possíveis contextos de representação. Os exemplos mais comuns de dados pessoais são:

- nome completo;
- nomes dos relativos, cônjuge, filhos;
- data e lugar de nascimento;
- endereço residencial;
- número de telefone (também celular);
- lugar de trabalho;
- dados biométricos (fotos, impressões digitais, imagens da iris, padrões de locomoção do corpo);
- vídeos e gravações de voz;
- números de documentos de identidade (passaporte, carteira de motorista, título eleitoral, etc);
- número de identificação de contribuinte;
- números de cartões de crédito;
- placa de carro;
- informações médicas, em particular genéticas;
- endereço e-mail (em muitos casos);
- endereço IP do computador ou outro dispositivo (em alguns casos).

Cada vez mais frequentemente, a informação sobre o lugar onde alguém encontra-se em um certo momento também é tratada como pessoal e sensível a revelação. A determinação deste lugar é possível graças a uma gama surpreendentemente vasta de inventos tecnológicos: telefones celulares, inclusive smartphones, carros equipados com GPS, dispositivos portáteis com acesso à Internet, redes sem fio, distribuição geográfica de endereços IP, tags RFID embutidos em documentos de identificação, cartões, crachás, pneus de carros, roupas, implantados em animais de estimação e até corpos humanos, a vigilância onipresente por câmaras em lugares públicos e sistemas de reconhecimento facial, de voz, de padrões de locomoção, de iris, etc. No Reino Unido, foi efetuada uma pesquisa que demonstrou que havia cerca de 1,85 milhões de câmaras naquele país em 2011, o que resultava em uma câmara para cada 32 cidadãos. Uma outra pesquisa estimou muito mais: 4,2 milhões[8]. A

7 Este é exemplo de um número de identificação de cidadão polonês, chamado PESEL. Ele é único, contém data de nascimento (6 primeiros dígitos), número serial (dígitos 7-9), sexo (décimo) e dígito de controle (undécimo). É muita informação para quem sabe que tipo de número é este (o contexto).

8 The Guardian de 2 de março de 2011, artigo "You're being watched: there's one CCTV camera for every 32 people in UK" de Paul Lewis (http://www.guardian.co.uk/uk/2011/mar/02/cctv-cameras-watching-surveillance, o carregado em 6 de junho de 2013).

corretude destas estimações é discutível, mas podemos afirmar que a vigilância por vídeo naquele país atingiu um nível realmente gigantesco. O artigo do qual foram extraídas estas estatísticas informa, também, que só no metrô de Londres havia 11 mil de câmaras, no mesmo ano.

Os dados pessoais podem ser processados (tratados). A mesma diretiva da União Europeia define estas operações da maneira seguinte, no Artigo 2º, inciso b):

"Tratamento de dados pessoais" ("tratamento"), qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registo, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição;

A compreensão da natureza dos dados pessoais, sua coleta, processamento, transferência, copiagem, uso, reuso, remoção, proteção, controle de acesso e outras ações é fundamental para a análise dos fenômenos ligados à privacidade dos usuários da internet. Infelizmente, como demonstramos em seguida, essa compreensão é rara e já o mesmo termo privacidade não é fácil de compreender e definir.

2.2. Coleta, transferência e agregação de dados pessoais

A coleta de dados pessoais existe há muito tempo. Hoje, os dados sobre cidadãos em forma de certidões de estado civil, documentos de identidade, dados tributários, etc. são coletados em todas as economias mundiais.

Os acervos clássicos de papel são difíceis de manter, agregar com outros e transportar para outros lugares. Esses fatos serviram mesmo como causas para o desenvolvimento da informatização, mas, ao mesmo tempo, constituíam uma barreira à violação da nossa privacidade. Simplesmente, sua fisicalidade (volume, peso, lugar onde se guardavam, métodos de acesso) dificultavam a revelação, deslocamento ou comparação com outros dados. Na época digital, não temos mais esses obstáculos. Dados e informação podem ser coletados instantaneamente, em volumes enormes, transferidos para qualquer parte do globo e agregados automaticamente. Além disso, uma informação representada digitalmente é praticamente indestrutível – uma vez coletada, ela pode ser copiada sem perda de qualidade e preservada indefinidamente. Esses são verdadeiros problemas da era digital que cada vez mais a faz merecer o sinônimo de "era de vigilância". Mas nem todos compartilham desta preocupação, ou seja, com as possíveis consequências desses problemas.

É preciso sublinhar que tais problemas não são ligados apenas à Internet, como muitos percebem. A nossa privacidade é, sim, ameaçada no que fazemos ao navegar na rede, pelo que fazem os donos de servidores, da infraestrutura da rede, agências governamentais, organizações e empresas, mas tais problemas devem ser cogitados em nível maior de abstração, pois a Internet é apenas mais um meio de comunicação e de produção de significados (um meio semiológico), enquanto o desenvolvimento técnico e a informatização são fatores mais abrangentes do que a rede por si só.

Em decorrência desse desenvolvimento, nós deixamos rastros digitais quase em cada passo: comprando com cartões de crédito, emprestando livros em bibliotecas, telefonando, dirigindo o carro, assistindo TV a cabo, solicitando emissão de documentos, solicitando créditos, fazendo consultas médicas, utilizando computadores e dispositivos portáteis, viajando e hospedando-nos em hotéis, e assim por diante. As câmaras onipresentes nas ruas, estádios, aeroportos, lojas etc. nos observam e os algoritmos de reconhecimento facial verificam se existimos como registros em vários bancos de dados. Nossas conversas são gravadas e verificadas com uso de técnicas de reconhecimento da voz. Nossos carros são fotografados nas ruas, suas placas reconhecidas por computadores. Em particular, os nossos telefones celulares viraram "espiões" potentes. A lista de métodos de invasão à nossa

privacidade continua crescendo o tempo todo.

Nos textos sobre a privacidade, aparecem frequentemente as citações do famoso livro "1984" de George Orwell, como "O Grande Irmão está te observando". Segundo análise literária prevalecente, esse livro refletia uma visão do desenvolvimento futuro do estalinismo[9]. Hoje, porém, vemos que certos elementos da realidade orwelliana surgem, também, nas sociedades tradicionalmente percebidas como democráticas e de livre mercado, além daquelas com sistemas políticos perversos.

2.3. Privacidade em busca da sua definição

A palavra *privacidade* aparece tanto na linguagem comum, como nas áreas de direito, psicologia, sociologia, filosofia, política, medicina, informática e outras. Mesmo sendo tão citada e aparecendo em tantas áreas, até hoje o conceito de privacidade não tem nenhuma definição fixa. O conceito não comporta nenhuma análise que seja definitiva e universalmente aceitável como tal. Parece que uma definição terminativa seja impossível, pois nenhuma tentativa de "axiomatização" da noção de privacidade parece ser completa. O primeiro obstáculo ao abordar cientificamente a noção de privacidade é que a sua percepção difere entre culturas, tanto no espaço, como no tempo. Existem línguas em que a palavra privacidade nem surgiu ainda (em russo, por exemplo).

A noção de privacidade inscreve-se no quadro da vida socioeconômica que depende do lugar geográfico e do momento histórico. Ou seja, mesmo dentro de cada cultura ou sociedade onde surge, o conceito da privacidade não é fixo, pois evolui no tempo, marcado por julgamentos de caráter moral e político, o que dificulta as chances de ser bem definido. Em consequência, o conceito da privacidade já foi dissecado e recomposto tantas vezes e de tantos modos que seu traço enciclopédico se assemelha a um "monstro cognitivo". Muitos trabalhos sobre privacidade – e a presente monografia não é exceção – começam reclamando que a privacidade sofre de excessiva polissemia, ou seja, de abuso de sentidos.

Em português, lexicalmente, o termo privacidade significa, na acepção que lhe confere o Dicionário Aurélio de 2004[10], *vida privada; vida íntima* ou *intimidade*, *intimidade pessoal ou de grupo definido de pessoas,* na edição de 2010[11]. Sobre a etimologia desse verbete, o Aurélio informa que ele vem do radical latino *privat* - que significa algo pessoal, íntimo, com acréscimo do sufixo *-(i)dade*, para acolher tradução do termo inglês *privacy.* A primeira edição do Aurélio, de 1975, não incluía o termo. Já a primeira edição do dicionário Houaiss (de 2001) define a verbete *privacidade* como: *"vida privada, particular, íntima"; USO: trata-se de anglicismo de empréstimo recente na língua (talvez na década de 1970)*.

Então, dado que a palavra "privacidade" no português contemporâneo é um anglicismo, é necessário pesquisar sua etimologia em inglês. Tracy Mitrano esclarece que a palavra inglesa *private* deriva do *privat* do inglês medieval, o qual, por seu lado, vem do latim *privatus,* que significa não pertencente ao Estado, não de ou em vida pública[12]. *Privatus* é oposto a *publicus* no sentido de pertencer ao *Populus Romanus* (Povo Romano). Cabe ressaltar que, já no nível etimológico, a palavra privacidade é colocada em dois contextos: o do direito e o da cultura anglo-americana. No inglês contemporâneo, *privacy* significa o que

9 Por exemplo, David Smith, Orwell for Beginners. O livro fala sobre as obras de Orwell, como: "A Revolução dos Bichos" que é uma paródia da Revolução Russa e do comunismo e de "1984" que é uma paródia chocante de um estado totalitário. Orwell foi um jornalista esquerdista e participou como soldado na Guerra Civil Espanhola. Ele presenciou a influência totalitária de Stalin e suas manipulações na comunidade dos comunistas espanhóis e percebeu ao que isso poderia levar.

10 Aurélio Buarque de Holanda, Novo Dicionário Aurélio da Língua Portuguesa, edição de 2004. p. 1632. Dicionário Aurélio 5ª Edição. http://www.dicionariodoaurelio.com/Privacidade.html (o carregado em 6 de junho de 2013).

11 Aurélio Buarque de Holanda, Dicionário Aurélio da Língua Portuguesa,, edição de 2010.

12 Tracy Mitrano, "Civil Privacy and National Security Legislation: A Three-Dimensional View", EDUCAUSE Review, vol. 38, no. 6 (November/December 2003): p. 52–62.

Raymond Wacks define da maneira seguinte:
No nível mais geral, a ideia da privacidade abrange o desejo de ser deixado sozinho, livre para ser si mesmo, desinibido e desconstrangido da intromissão dos outros[13].

A confusão em torno do termo privacidade vem, também, do fato de que ele pode se referir a outros conceitos semelhantes ou dele integrantes, tais como:

- isolação ou separação – estado ou desejo de ficar afastado física ou figurativamente;
- intocabilidade – estado ou desejo de não ser tocado física ou figurativamente;
- anonimato – estado ou desejo de ficar anônimo ou incógnito (literalmente sem nome ou sem possibilidade de se identificar esse nome);
- confidencialidade – indisponibilidade de informações percebidas como sensíveis a divulgação;
- seguridade – nível de proteção contra algo ou alguém;
- intimidade – relação interpessoal muito próxima (íntimo é frequentemente utilizado no sentido de pessoal ou privado);
- *proteção de dados pessoais* – essa é uma acepção relativamente nova do termo, pelo menos no que diz respeito aos dados eletrônicos, sendo semelhante à confidencialidade.

Certamente esta lista não é completa, nem pretende ser. Os conceitos supramencionados se conectam à noção de privacidade em seus vários possíveis contextos, mas não ocupam dentro dele posição fixa. O que é percebido como privado depende, entre outros fatores, do que é compreendido como público. Essa contraposição de privado versus público sempre depende da cultura. Ao mesmo tempo, essa distinção é dinâmica dentro de cada cultura. Adicionalmente, esses componentes da noção de privacidade podem sobrepor-se, podem ser considerados como direitos (tanto legais como naturais), como condições, como valores, como interesses, por vezes definíveis negativamente (ou seja, por suas violações) ou qualquer combinação destes, donde a "neblina" que encobre conceituações de privacidade.

Wacks indica que durante as últimas três décadas (desde os anos 80) a privacidade foi estendida para integrar questões de natureza moral, que ele chama de decisionais, como: aborto, contracepção, preferências sexuais, pornografia e outras. Do seu ponto de vista, tem ocorrido uma conjugação equivocada do conceito da privacidade com os conceitos de liberdade e autonomia. O surgimento desses novos elementos conectados à noção faz com que as discussões sobre privacidade obtenham caráter moral[14], que a tornam ainda mais difícil de lidar na esfera do Direito.

Num dos contextos em que a privacidade emerge, porém, sua pertinência não causa disputas. Este é o contexto social. Para cogitar-se a privacidade precisamos de mais do que um indivíduo, pois não faz sentido falar em privacidade de um indivíduo sem suas relações com a sociedade e com outros indivíduos. Nelas é onde ocorre a contraposição entre o público e o privado.

Essa contraposição é muito antiga. Foi Aristóteles o primeiro que cogitou a distinção entre a atividade política, que pertencia à esfera pública *(polis)*, da que pertencia à esfera doméstica e da família *(oikos)* e daquilo que é próprio ao homem *(idion)*[15]. Arendt fala da suprema importância que a vida pública (política) teve nos tempos antigos da Grécia e Roma. Em particular, *privatus* em Roma significava o mesmo que hoje significa o "privado" em português, idioma que, a propósito, é uma língua românica. O sentido aqui era o de ser privado ou desprovido de algo; de algo significativo, que pode estar mesmo entre as mais elevadas capacidades humanas. Quem vivia apenas a vida privada, como escravos ou

13 Raymond Wacks, "Privacy, A Very Short Introduction", Oxford University Press, 2010, p. 30.
14 Ibid., p. 30-31.
15 Hannah Arendt, "The Human Condition", p. 23.

bárbaros, nem era considerado cidadão, e em alguns casos nem mesmo humano[16]. Ao mesmo tempo, os "verdadeiros homens" precisavam do privado, que servia como abrigo à vida pública. Na esfera privada, eles podiam descansar e restituir as forças vitais para voltar de novo à vida pública e servir melhor ao Estado. O privado, porém, era tratado como refúgio temporário e não denotava o sentido de íntimo. Esse sentido, do privado como íntimo, começou a aparecer na Roma Antiga apenas em seu período tardio[17]. O melhor exemplo preservado do sentido originário da palavra "privado", denotando "desprovido de algo significativo", seria na sua correspondente em inglês, *private*, na acepção do substantivo que significa "soldado", i.e. alguém desprovido de status na hierarquia militar.

Todavia, a separação dos domínios público e privado ampliou-se. Wakcs indica como motivo para tal o desenvolvimento do pensamento político e jurídico[18]. Surgiram os estados nacionais, em que o domínio público ficou delimitado de uma maneira mais abrangente e mais clara. Ao mesmo tempo, os monarcas e os parlamentos precisavam da liberdade e da separação do público para criarem as leis de uma maneira soberana. As leis que regularizam a vida social e econômica em estados modernos naturalmente tendem a separar a esfera privada da pública.

A primeira tentativa significativa de esclarecer o termo "privacidade" ocorreu nos EUA, em 1890, na área do Direito. Samuel Warren e Louis Brandeis publicaram o famoso ensaio intitulado *The Right to Privacy* em 1890[19] que referiu-se ao invento da fotografia e seu uso na imprensa, a qual na época se tornava uma mídia de massa. Foi neste texto que teve origem a famosa, lacônica definição da privacidade como "*the right to be left alone*" (o direito de ser deixado sozinho). A imprensa detinha a possibilidade – nova então – de fotografar e citar os indivíduos sem consentimento destes, e de divulgar esse material em escala nacional. Para os autores, tal divulgação constituía uma injúria permanente aos indivíduos expostos. Essa prática, conforme os autores, causava dano moral dentro dos padrões de convivência social (da época). A conclusão principal do ensaio foi:
"Os indivíduos terão a proteção plena em pessoa e em propriedade como um princípio tão antigo, como a lei comum; mas foi descoberto ser necessário, as vezes, redefinir a natureza exata dessa proteção. As mudanças políticas, sociais e econômicas implicam o reconhecimento de direitos novos e a lei comum, em sua juventude eterna, cresce para corresponder às demandas da sociedade."[20] [tradução do autor].

Assim, os autores efetivamente proclamaram a possibilidade e mesmo a necessidade de se reformular a definição de privacidade conforme o desenvolvimento social. Isso, na verdade, significa a admissão do fato de que qualquer definição fixa da privacidade na área do Direito seria impossível, pois o Direito reflete o estado dinâmico das relações político-econômicas e socioculturais em uma determinada sociedade e em um momento dado. Cabe citar da fundamentação daquela manifestação de Warren e Brandeis pois ainda soa atual:
"A imprensa ultrapassa, em cada sentido, os limites óbvios da propriedade e decência. A fofoca não é mais um recurso dos vaidosos e viciados, mas se tornou um negócio, que é procurado com engenho, mas, também, imprudência. Para satisfazer o gosto lascivo, os detalhes das relações sexuais são divulgadas nas colunas dos jornais diários. A intensidade e a complexidade da vida da civilização em avanço criaram a necessidade de certo afastamento do mundo, e o homem, sob a refinada influência da cultura, tornou-se mais sensível à publicidade e, assim, a solitude e a privacidade tornaram-se mais essenciais para

16 Ibid., p. 27.
17 Raymond Wacks, "Privacy, A Very Short Introduction", Oxford University Press, 2010, p. 32.
18 Ibid., p. 33.
19 "The Right to Privacy", Samuel Warren e Louis Brandeis, Harvard Law Review, Vol. IV, No. 5, 15 de dezembro de 1890. O texto completo pode ser encontrado em http://www.harvardlawreview.org/media/pdf/vol126_cohen.pdf (o carregado em 6 de junho de 2013).
20 Ibid., p. 193.

o indivíduo; mas o empreendimento e a invenção modernos, através das invasões à sua privacidade, subordinaram-no à dor mental e angústia muito maiores daqueles que o poderiam infligir por mera injúria corporal."[21] [tradução do autor].

Provavelmente, Warren e Brandeis ficariam sem palavras se fossem apresentados ao mundo da mídia contemporânea e da Internet. Uma observação importante de DeCew sobre aquele seminal ensaio diz:

"[...] os autores consideraram a privacidade como já integrada na Common Law (Direito Comum)*, protegendo o princípio de "My home is my castle"* (Minha casa é meu castelo)*, mas a tecnologia nova provocou a urgência e importância do reconhecimento explícito e separado dessa proteção sob o nome da privacidade. Eles sugeriram que as limitações do direito poderiam ser determinadas analogamente às leis sobre a calúnia e difamação e não permitiriam, por exemplo, prevenir as publicações das informações sobre os políticos concorrendo aos cargos públicos. Assim, Warren e Brandeis fundaram o conceito da privacidade que veio a ser conhecido como o controle sobre a informação sobre si mesmo."*[22] [tradução do autor]. Em seguida, DeCew frisa o papel de Alan Westin, um professor do Departamento da Lei da Columbia University e perito na área da privacidade, que já em 1967 aprofundou este conceito jurídico da privacidade, e a definiu como *"direito de um individuo de decidir como e até que nível os dados pessoais podem ser revelados a outros sujeitos".* Essa formulação se adéqua a avanços tecnológicos que permitiram a coleta e processamento digital de dados pessoais, mas talvez não o suficiente (como pode uma pessoa "decidir até que nível" dados sobre si, coletados por terceiros, podem se tornar mais pessoais através de integração com outros dados, estes coletáveis fora do seu controle?) Simplesmente, os métodos de invadir a paz de alguém multiplicaram-se e ficaram altamente elaborados e sofisticados.

Essa conceituação, baseada no controle sobre a divulgação de dados pessoais (não apenas por um individuo sobre si mesmo, mas por qualquer outra entidade ou sujeito), é de suma importância na época digital, quando as discussões sobre a privacidade são, antes de mais nada, ligadas às ameaças viabilizadas pela tecnologia moderna, que trouxe incontáveis possibilidades de se invadir, limitar, falsificar ou subverter esse controle. Isto porque a pessoalidade do dado depende do contexto, e este, de possíveis agregações com outros dados, que atuam como metadados para representar informação (que pode ser invasiva), num cenário onde as possíveis agregações podem ser automatizadas e multiplicadas.

Cabe ressaltar que a publicação do ensaio de Warren e Brandeis não recebeu uma resposta imediata por parte do poder judiciário norte-americano, mas a maior prazo. Pois este logo começou a expandir a defesa da privacidade, lastreando precedentes que iriam influenciar futuros julgamentos naquele pais[23].

Conforme DeCew, em geral, as obras sobre privacidade na área do direito dividem-se em duas categorias: reducionista e coerentista. A abordagem reducionista, em princípio, nega a relevância do que chamamos de privacidade, reduzindo-a a aspectos de outros direitos ou interesses, como a proteção à integridade corporal, aos direitos de propriedade, proibição de vigilância, etc. Essa visão tem caráter crítico em relação ao que seria privacidade. A abordagem coerentista, por seu lado, busca preservar a separação do conceito de privacidade, pois os interesses presumidos na noção de privacidade são percebidos como coerentes e de valor fundamental[24].

Marcella e Stucki, em *Privacy Handbook,* indicam várias debilidades e limitações nas definições da privacidade como direito. Eles indicam que a privacidade é algo individual, que

21 Ibid., p. 196.

22 DeCew, Judith, "Privacy", The Stanford Encyclopedia of Philosophy (Fall 2012 Edition), Edward N. Zalta (ed.), URL = http://plato.stanford.edu/archives/fall2012/entries/privacy/ (carregado em 6 de junho de 2013).

23 Ibid.

24 Ibid.

cada um de nós percebe de maneira mais ou menos diferente:

For every person in society, for every position, belief, role or responsibility, each will have his, her, their own view or perception of what is and what should be private and what privacy (or the concept of privacy) means to them.[25]

Os autores acrescentam:

O conceito de "direito" é um caminho problemático para começar, pois "direito" parece ser certo padrão absoluto. O que é pior, é muito fácil confundir os direitos legais, por um lado, com os direitos naturais e morais, por outro lado.[26][tradução do autor].

Eles afirmam que a privacidade é mais um interesse. Se abrirmos este caminho, vemos que a privacidade é então um conjunto de interesses de uma pessoa ou pessoas, que se cruzam com interesses de outras pessoas, entidades ou da sociedade como um todo. Eles indicam que a privacidade de um não pode dominar ou invadir a privacidade de outro ou contrariar os interesses sociais[27].

Vale a pena mencionar que a ideia da proteção à privacidade pela lei tem também seus oponentes. Catherine Mackinnon, partindo das posições feministas, afirma que as tentativas de se proteger a privacidade no âmbito jurídico ou em outras esferas podem disfarçar o sofrimento de mulheres e outros que têm sua autonomia corporal violada no ambiente familiar.[28]

Um outro exemplo são pesquisas médicas, como o famoso caso da linhagem imortal de células cancerígenas (HeLa) obtidas de Henrietta Lacks em 1951, sem consentimento dela e da sua família[29]. A Sra. Lacks morreu no mesmo ano, mas graças a essas células (a paciente fora diagnosticada de carcinoma de células escamosas de cérvix), apareceram muitas dissertações e avanços em várias áreas das ciências médicas, a genética em particular e, obviamente, várias instituições e pessoas ganharam muito dinheiro. Havia muitas vozes contra este tipo de prática, como violadora da privacidade (integridade corporal e dignidade humana) e até denúncias de racismo (a Sra. Lacks era de uma família pobre da origem afro-americana). Temos aqui um exemplo claro de como uma violação à privacidade pode ter uma utilidade médica em escala mundial e, ao mesmo tempo, como ela pode ser dramaticamente complexa quando cogitada em vários possíveis contextos.

2.4. Visão do autor sobre a privacidade

Existe em torno das pessoas uma área que podemos chamar de área de privacidade física. Seu perímetro, ou seja, a questão de onde ela se situa e até onde ela se estende, varia para cada pessoa, mas ela existe e até foi cientificamente definida de ter, em média, 45 cm (íntima) até 120 cm (pessoal)[30] (neste texto vamos tratá-las junto como "físicas"). Se alguém, ao se aproximar, fica fora desse perímetro, esse alguém não invade a nossa área da privacidade física. Essa abordagem física da privacidade refere-se ao que podemos tratar como isolamento corporal: a integridade que um indivíduo sente quando isolado de outros

25 Albert Marcella Jr., Carol Stucki, "Privacy Handbook, Guidelines, Exposures, Policy Implementation, and International Issues", p. 2.

26 Ibid., p. 53.

27 Ibid., p. 53-54.

28 Catharine A. MacKinnon, "Reflections on Sex Equality under Law", The Yale Law Journal, Vol. 100, No. 5, Centennial Issue (Mar., 1991), pp. 1311.

29 Robin McKie, The Observer, "Henrietta Lacks's cells were priceless, but her family can't afford a hospital", 4 de abril de 2010, também: Paul Harris, The Observer, "Final twist to tale of Henrietta Lacks, the woman whose cells helped the fight against cancer", 31 março de 2013.

30 Edward Hall, "The Hidden Dimension", 1966 (o autor definiu as "bolhas de reações pessoais" de quatro raios: íntimo, individual, social e público, cada um com duas fases: próxima e distante (medidos em centímetros até pés). Um resumo desta questão pode ser encontrado na Wikipédia inglesa, no artigo "Personal space", http://en.wikipedia.org/wiki/Personal_space (carregado em 22 de junho de 2013). Um exemplo em português é o artigo: *Como perceber o desconforto no abraço?* de Sérgio Senna Pires, sob o endereço: http://linguagemcorporal.net.br/blog/proxemica/desconforto-no-abraco/ (carregado em 6 de junho de 2013).

seres, pessoas ou objetos capazes de invadir esse espaço. Regra geral, não gostamos de ser espremidos por uma multidão de pessoas, ou quando algum estranho inesperadamente aproxima-se demais de nós. Ficamos alertas e incomodados quando, por exemplo, algum estranho de repente nos toca, sem nosso consentimento. Ao contrário, se um médico nos toca durante uma consulta isso normalmente não causa tal reação, embora possa, se o médico fizer isso de uma maneira incomum, que não corresponda à nossa experiência ou expetativa sobre formas de contato legítimas com essa classe de profissionais. Ou, quando somos tocados por pessoas de nossa intimidade, as quais já nos são "próximas": cônjuges, crianças, parentes ou amigos. Normalmente gostamos disso e o elemento da surpresa pode até aumentar a satisfação desse contato físico.

Esse aspecto ou elemento da privacidade corresponde à separação inicial entre papéis que a psique do indivíduo busca atribuir, com relação aos que possam interagir com o seu próprio corpo, entre aqueles seres ou coisas que lhe são "íntimos" e os que lhes são "não-íntimos" ou "estranhos". Podemos chamar o exercício dessa separação de autonomia corporal, e a área da privacidade física poderia então ser entendida como espaço que o indivíduo demarca para o exercício da sua autonomia corporal.

O que importa nesse momento da nossa análise do conceito de privacidade é reconhecer que existe, para cada indivíduo, certa zona que pode ser por ele considerada como invadida mediante a presença e/ou determinada atitude de outra pessoa, coisa ou outros fatores (cheiro, barulho, etc.).

Normalmente, esse elemento é mais um ponto de partida para substanciar a definição de privacidade quando as tentativas de fazê-lo a partir de conceitos pretensamente mais fundamentais, como valor, direito, condição, interesse, etc. ficam incompletas, ao darem ensejo a reflexões sobre a variedade praticamente ilimitada de contextos que permitem cogitar distintas acepções ou aspectos desse conceito. Depois de falhar em enumerar esses contextos, os autores que seguem essa abordagem buscam o caminho de eliminá-los, um por um, para tentarem chegar a algo suficientemente primordial ou abstrato, com o qual possam substanciar uma definição satisfatória e útil da privacidade.

Parece-nos que, ao definir a privacidade, o método indutivo é de certo modo insatisfatório, mas isso, a nosso ver, não deveria ser o "fim da linha". O problema está no número gigantesco de aspectos lastreáveis em fatos e premissas, que são por si mesmos discutíveis e possivelmente contraditórios entre situações distintas. Quando o método indutivo falha, recorra-se ao método dedutivo. Infelizmente, também esse método parece falhar. Tentando dissecar a noção de privacidade a partir de possíveis consequências, estaremos a cada passo eliminando elementos que não podem ser eliminados totalmente. O conceito começa a ser diluído, cai na definição de outros termos e, consecutivamente, leva a uma definição sem abrangência, unidade e/ou utilidade satisfatórias. É possível, então, que estejamos diante de um conceito essencialmente metafísico, relacionado à natureza do ser humano consciente.

Voltando então à sede desse "ser", dependendo da constituição psíquica do individuo, que pode estar ligada à cultura e ao ambiente social, e também, à predisposição da pessoa em um momento dado, a extensão e intensidade de sua autonomia corporal podem variar, mudando o perímetro da área da privacidade física e/ou a avaliação de riscos de ameaças, de eventual invasão e possíveis consequências, que calibram suas reações a ela. Nossa avaliação do risco de invasão (seus critérios, incluindo o perímetro da área a ser protegida), a intensidade da nossa resposta, etc., são funções de muitas variáveis, dificilmente enumeráveis de forma completa. Isso já sinaliza que a reação (do indivíduo a um risco iminente à sua autonomia corporal) não precisa ser lógica, adequada à situação, mensurável ou mesmo objetivamente definível. A pressuposição é que estamos lidando com alguma coisa inerentemente psicobiológica, relacionada, neste caso, aos papéis sociais que o indivíduo se

atribui para lidar com "íntimos" e com "estranhos", e às estratégias que emprega para atribuir esses papéis (de "íntimos" e "estranhos") a terceiros.

Podemos lembrar que existem – e sempre existiram – diferenças nos rituais cotidianos de se saudar ou cumprimentar, entre as várias culturas. Os povos do Norte da Europa não são muito "abertos" nesse sentido, enquanto, por exemplo, os povos latino-americanos demonstram uma cordialidade significativamente maior. Certos gestos ou comportamentos, como beijar, abraçar ou dar palmadas nas costas das pessoas desconhecidas, inclusive mulheres, podem ser consideradas aceitáveis e até normais em certas culturas, enquanto em outras podem causar estranheza, repugnância, sinal de má educação ou até de crime. Os parentes japoneses, por exemplo, não demonstram muita afetividade em relação às suas crianças e vice-versa, o que é absolutamente normal naquela cultura. No Japão, a interação com pessoas estranhas é ainda mais restrita. As invasões da área da privacidade física podem ser tratadas como algo por definição inaceitável e condenável socialmente. Nas culturas dos povos muçulmanos, os padrões da interação pessoal expressadamente excluem os contatos dos homens com as mulheres "alheias". Tocar a mão de uma mulher, mesmo de uma maneira inocente e cordial, o que é relativamente comum na Europa e nas Américas, pode ser tratado como algo absolutamente inaceitável e até sujeito a punição. É interessante ressaltar que a diplomacia, que por natureza é internacional e transcultural, pressupõe a necessidade de interação entre os representantes de várias culturas e nações. Os diplomatas experientes dos países ocidentais, ao serem apresentados a um casal muçulmano, sempre apertam a mão do homem, o que parece ser culturalmente aceitável em todo o mundo, mas se abstêm de fazer o mesmo com a esposa do seu colega. Se, por gentileza inocente, um diplomata não muçulmano inexperiente estende a mão a essa mulher, ela cobre a mão com um pedaço de tecido do seu vestido para não ofender um representante de outra nação rejeitando esse gesto cordial, mas também para não violar as normas da sua própria cultura e não interferir com os sentimentos do seu marido. Os diplomatas muçulmanos experientes, por sua vez, também entendem a complexidade intercultural desses momentos e não reagem. Isso mostra que a área da privacidade física nem sempre é controlável apenas pelo próprio indivíduo. Ao mesmo tempo, podemos assinalar que existem mecanismos de entendimento intersubjetivo que funcionam mesmo com diferenças culturais significantes e surpreendentes. Infelizmente, a aplicação desses mecanismos não é comum fora da área da diplomacia.

As origens e as diferenças entre os níveis da cordialidade e da "abertura emocional" aceitáveis em várias culturas não constituem objeto da presente monografia, mas são aqui citadas para ilustrar a complexidade da atribuição de papéis sociais relacionada à privacidade. Neste sentido, mais uma observação parece pertinente. Quanto mais boreal a cultura humana, menos "aberta" ela tende a ser. Um dos caminhos interessantes para pesquisar esta tese é a atividade solar anual nas áreas geográficas correspondentes. A presença de claridade e calor evidentemente influencia a atividade humana. As condições climáticas e topográficas influenciam a nossa vida de numerosas maneiras.

Existem obras interdisciplinares em psicologia e arquitetura que mostram que o jeito de organizar o espaço arquitetônico nas culturas antigas dependia das percepções de privacidade (reclusão de casas e seus arredores)[31]. Isso continua valendo, hoje em dia. Buscamos, também, a reclusão, pois isso é algo natural em várias situações. Aqui, aparecem mais elementos fundamentais para a privacidade – família e casa (abrigo).

Antes de incluir mais estes dois elementos na nossa análise, já podemos observar que, mesmo partindo das observações evidentemente primordiais sobre a privacidade, como sua dimensão física e sua manifestação em autonomia corporal, logo flutuamos sobre os domínios da psicologia, filosofia, cultura, etnologia, direito e, também, religião.

Diante da possibilidade de ameaças e invasões de natureza física, observamos que os

31 Por exemplo, Irwin Altman, "The environment and social behavior". Monterey, CA: Brooks/Cole (1975).

comportamentos supramencionados têm um caráter instintivo, de impulso reflexivo. De certo modo, sempre reagimos assim quando alguém viola o nosso senso da privacidade física. No caso de um assalto, agimos instintivamente para nos defender de morte, lesão ou perda de um objeto de valor. E em casos de uma invasão menos grave, também, agimos afastando-nos do agente invasor e/ou expulsando-o da nossa área de privacidade, verbalmente ou mesmo fisicamente. Vale a pena diferenciar essas duas atitudes: o primeiro caso seria, por exemplo, uma disputa, e o segundo, uma escaramuça. Calar-se e não reagir também integra o leque das possíveis reações. Por exemplo, durante um assalto a mão armada, este padrão de comportamento pode ser o mais racional e saudável. Então, a falta de ação pode também ser uma reação. Já um outro exemplo, em que tal atitude teria o caráter diametralmente oposto, seria a violência doméstica. Não reagir nessa situação, o que infelizmente parece ser conduta corriqueira, significa permitir que a transgressão se perpetue, por vezes com o possível atenuante da vítima não ter a possibilidade de reclamar[32].

O nosso isolamento como seres corpóreos, ou nosso impulso para assim mantê-lo quando em risco, influencia nossa forma de pensar sobre outras modalidades de isolamento, e o elemento instintivo desse pensamento continua existindo, ou deve existir, em todos os possíveis níveis de abstração onde o mesmo impulso contra possíveis ameaças pode atuar. Solove[33] aponta que as reações a violações da privacidade frequentemente têm caráter semelhante ao efeito patelar (*knee-jerk form*), o que confirma a existência do elemento instintivo na privacidade corporal (e familiar, como a proteção de crianças).

Então, a privacidade, como impulso seletivo pela reclusão, começa pelo isolamento corporal e, em níveis seguintes, estende-se à família, conjunto mais nuclear de seres humanos "íntimos", e depois à casa, espaço físico onde esses seres se abrigam e podem juntos se isolar de potenciais ameaças. Até aqui, os desejos, vontades, hábitos e práticas relacionados à privacidade não nos diferenciam muito do mundo animal, do qual fazemos parte, sinalizando uma natureza primordial da mesma, sua *naturalidade*[34].

A proteção corporal de nós mesmos, e a de quem nós cuidamos, é algo instintivo, fato que cria a oportunidade para se afastar a ideia de que o conceito de privacidade seja algo puramente cultural ou humano. Ela não é algo apenas humano: como algo baseando em instinto, a privacidade é comum no mundo animal, manifesto no impulso de proteção ao corpo de um indivíduo, à sua família e à área onde estes melhor se abrigam. Garfinkel diz: *Sem habilidade de prevenir ou controlar invasões, a vida, como tal, não pode existir. Os organismos utilizam suas paredes celulares para proteger sua integridade corporal contra invasões. Nós, os humanos, dependemos da nossa pele, casas ou cercas para proteger nossa integridade ou privacidade*[35] [tradução do autor].

Devemos sublinhar que a privacidade humana não pode ser reduzida ao instinto – ela não é instinto, pois ela evolui dentro e junto com as culturas. Ela apenas possui elementos instintivos, principalmente na defesa corporal e familiar. Cabe ressaltar, que o caráter instintivo da privacidade não deve ser cogitado como algo inconsciente em humanos. É aqui que podemos justamente diferenciar os comportamentos humanos dos demais animais. Como seres capazes de pensar de maneira abstrata, somos capazes de perceber, estudar e controlar nossos instintos. Somos conscientes da nossa existência e da força em nós e em todo o mundo animal. Porém, deve-se admitir que a ênfase no caráter instintivo da privacidade em humanos

32 São estes aspetos que preocupam a já citada Catherine Mackinnon. Vale pena conhecer os pensamentos dela, por exemplo na Wikipédia inglesa: http://en.wikipedia.org/wiki/Catharine_MacKinnon (carregado em 22 de junho de 2013).

33 Solove Daniel J., "A Taxonomy of Privacy", University of Pennsylvania Law Review, vol. 154, no. 3, de Janeiro de 2010.

34 O primeiro capítulo do livro "Privacy and Freedom" de Alan Westin (1967) dedica-se à "Privacy in the Animal World."

35 Garfinkel Simson, "Database Nation, The Death of Privacy in the 21st Century", p. 321.

pode ser discutível. Tal ênfase pode soar como algo "animalista" e, por isso, talvez inadequado. Ela pode, por exemplo, contradizer nossa posição como "coroamento" da criação, proclamada pela religião, pelo cristianismo em particular, de uma maneira que fora dela é narcisista.

Talvez, seja melhor afirmar que este elemento instintivo da privacidade em humanos seja guiado pela intuição, a qual, ao ver do autor, é mais uma ferramenta que se baseia em algo inato, geneticamente herdado, mas enriquecido com a experiência adquirida na vida e pela cultura. Eis que assim voltamos ao início: não podemos afirmar que a intuição seja algo puramente humano, pois existem fatos e estudos que contradizem essa tese. Muitos animais são capazes de prever desastres naturais, como terremotos. Enquanto os humanos, ao que parece, perderam estas habilidades no decorrer da evolução, mas tendem a readquirí-las com o auxílio da tecnologia. Dessa forma, ciência e tecnologia humanas, de certo modo, oferecem extensões ou próteses aos nossos instintos naturais (animais).

A estes três elementos que compõem, até agora, a nossa abordagem à noção da privacidade – *corporal, familiar* e o *territorial* (que nos parecem universais no reino animal) – devemos acrescentar mais dois – o de *comunicação* e o *informacional*.

Aqui, pode parecer que esses dois elementos, em oposição aos três primeiros, seriam restritos aos humanos. Mas em certo nível de abstração, também esses elementos podem ser identificados em comportamentos de animais. Os animais comunicam-se entre os membros da mesma espécie e entre espécies. Para isso, eles usam uma variedade enorme de linguagens em que símbolos desempenham papel representacional: sons, cores, luzes, cheiros, movimentos, poses, atitudes, sinais químicos e elétricos[36]. Um dos motivos fundamentais para tais elementos parece ser a proteção do corpo, da família (filhotes), do rebanho, do território (de caça e coleta que sustenta o rebanho), do ninho, etc. com objetivo puramente darwinista de reproduzir-se. A dimensão informacional, inclusive no que diz respeito a proteção dela, também não é algo puramente humano. Todo animal parece que aprende ou, simplesmente, coleta informações e, com base nelas, constrói "conhecimentos" necessários para sobreviver, reproduzir-se e proliferar. Os animais territoriais não só defendem seus abrigos, mas frequentemente delimitam seus territórios deixando os sinais que os outros animais podem ler. Por exemplo, os gatos (machos) marcam suas áreas com urina e, também, instintivamente enterram seus excrementos para esconder a informação sobre sua presença de seus predadores naturais. A diferença entre os animais e humanos com relação ao elemento comunicacional e informacional da privacidade vem da complexidade da cultura e da tecnologia que os humanos desenvolvem e repassam de geração a geração por meio da educação. Com respeito a elas, a diferença entre humanos e outros animais é de escala e complexidade destas atividades. Cabe ressaltar que, por enquanto, a Natureza é uma campeã inquestionável na área de camuflagem e criptografia de sinais na presença de predadores e suas vítimas.

Os elementos comunicacionais e informacionais da privacidade em humanos sempre desempenharam papéis essenciais. A escuta sigilosa de conversas, intercepção de correspondência, o rastreamento e a coleta de informações sobre indivíduos e/ou organizações de todos os tipos acompanham a humanidade desde os primórdios das suas estruturas sociais. O que mudou em tempos modernos e pós-modernos é a escala, complexidade e rapidez destes empreendimentos.

Uma das grandes revoluções na área da comunicação – o invento do telégrafo e, particularmente, do telefone – ampliou as possibilidades de humanos se interconectarem entre quaisquer lugares do mundo onde se estendeu a rede de cabos de cobre. Hoje, temos ainda cabos de fibra ótica e satélites de comunicação. A Internet, mesmo que utilize cada vez mais essas novas vias de comunicação, em grande parte de sua capilaridade continua baseando-se

36 Neste nível de abstração, podemos afirmar que até as plantas e animais (insetos, por exemplo) são capazes de se comunicar entre si.

nesta rede da era anterior (fios de cobre), embora tal situação esteja mudando com a evolução dos dispositivos móveis de comunicação sem fio.

A transmissão modulada por sinal elétrico analógico via cabos de cobre é muito fácil de ser grampeada para escuta clandestina. O invento da gravação magnética permitiu o registro e armazenamento das grampeagens da comunicação telefônica. Noticiários sobre grampos ilícitos de conversas telefônicas continuam, parecendo cada vez mais generalizadas. Além da polícia e das agências de segurança estatais e privadas em busca dessas conversas, até veículos da mídia corporativa em busca escândalos para vender melhor seus espaços de propaganda aos anunciantes. Um exemplo recente é o escândalo de grampos telefônicos no Reino Unido[37]. Naturalmente, essas práticas aparecem também na área da disputa pelo poder político (famoso caso de *Watergate* e sucedâneos, como a violação do painel do Senado no Brasil em 2001).

A coleta em massa de dados sobre pessoas físicas e jurídicas também não é algo que só surgiu na era digital. Órgãos de Estado contemporâneos coletam dados em forma de certidões de estado civil, endereços residenciais, registros de contribuintes, registros de antecedência criminal, dados de caráter estatístico e vários outros. Cabe ressaltar, porém, que os dados estatísticos em formato final não devem conter, por definição, elementos que possam, como ou com metadados, permitir identificar os indivíduos sendo pesquisados. Mas tais dados frequentemente contêm elementos que os tornam pessoais e identificáveis, em particular na etapa de coleta bruta, como no caso do CENSO no Brasil. Assim, o adjetivo "estatístico" deve ser atribuído aos dados cuidadosamente, apenas após uma verificação dos mesmos contra a variedade de possíveis contextos de interpretação e modos de aplicação, nos quais alguns dados poderiam servir de metadados para tornar outros pessoais e identificáveis.

As agências de defesa, de segurança, polícias etc. criam acervos gigantescos de dados pessoais para buscar ameaças à vida social e estatal. Um exemplo recentemente discutido é a construção de um centro de dados gigantesco da National Security Agency (NSA), no Utah, nos EUA, cujo orçamento é avaliado em 2 bilhões de dólares.[38] Os bancos comerciais tendem a conhecer tudo o que seja possível sobre a capacidade creditícia de seus clientes. As seguradoras fazem o mesmo, buscando informações que possam melhorar estimativas individualizáveis de possíveis riscos e indenizações. Para as seguradoras, dados médicos, em particular os de natureza genética, de um individuo e de seus ancestrais podem ser de grande valor, o que causa muitas preocupações legais e morais com respeito à coleta e armazenamento dos mesmos. A maioria das empresas buscam conhecer o quanto podem seus clientes. Todos com motivos aparentemente meritórios e justificados. Os governos poderiam melhor planejar suas ações e proteger seus cidadãos. A medicina poderia melhor enriquecer o acervo de tratamentos de doenças e avaliar os riscos de epidemias. As instituições financeiras poderiam evitar fraudes e créditos demasiadamente arriscados. Seguradoras e outras empresas poderiam servir melhor seus clientes, modificando suas estratégias para prestar serviços, produzir, vender e comunicar-se com os consumidores através da publicidade.

Por que, então, a coleta de dados sobre nós causa tantas preocupações, hoje em dia? Essa pergunta não é tão difícil como parece. Simplesmente, a informação é igual a poder onde ela é assimétrica (ou seja, poder para quem a detém, sobre aqueles para quem a mesma informação seria útil ou importante se as tivessem). E a história da humanidade demonstra claramente que o excesso de poder, concentrado em poucos, leva a situações sangrentas. O excesso da oferta de dados pessoais (que contextualizados representam informação sobre os

37 A Wikipédia inglesa publica o artigo muito detalhado intitulado "News International phone hacking scandal Phone-hacking scandal", http://en.wikipedia.org/wiki/News_International_phone_hacking_scandal (carregado em 6 de junho de 2013).

38 Bamford James, artigo "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)" no Jornal Wired, de 15 de março de 2012, http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1 (carregado em 6 de junho de 2013).

respectivos indivíduos) gera o possível excesso de poder. Como seres humanos, desejamos paz em nossos abrigos íntimos, e o excesso de poder não o garante, antes o desestabiliza. Embora os concentradores de poder sempre justifiquem a necessidade de ampliar o seu, manipulando a consciência da multidão acerca de riscos, "deslocando" a percepção do foco do perigo e distorcendo as possíveis escalas psicológicas que implicitamente usamos para avaliar riscos subjetivamente, buscando inimigos de fora que possam substituir o real perigo nessa concentração excessiva, o que leva à intolerância sob escudo de proteção contra algo ou alguém supostamente hostil, mas realmente não tão perigoso ou mesmo imaginário[39]. Este parece ser um fenômeno constante de manipulação psicológica em sociedades complexas, que poderíamos classificar como dimensão psicológica do contrato social hobbesiano[40].

Recapitulando, a privacidade, conforme propomos conceituá-la aqui, possui os seguintes aspectos ou componentes:

- corporal;
- familiar;
- territorial;
- comunicacional;
- informacional.

Os quais se juntam e se sobrepõem formando um domínio complexo, dinâmico e interligado com outros domínios subjetivos e intersubjetivos. Isso ocorre dentro de vários possíveis contextos, compostos de uma dimensão cultural, uma social e uma individual. A intenção ou intensidade das medidas de proteção à privacidade, ou as expectativas de como ela deve ser protegida por leis ou normas de conduta, dependem, no indivíduo, inclusive do seu gênero e idade. Aparentemente, temos menos exigências em relação a nossa privacidade quando jovens. Elas crescem na medida que ficamos mais maduros, responsáveis por nós mesmos e por nossas famílias, pois com elas ajustamos e calibramos nossos papeis sociais, e afinamos estrategias de comportamento para exercê-los. Alguns autores definem o sexo não apenas como uma categoria biológica, mas também como um papel social[41].

Essa dimensão individual faz com que a privacidade, como algo pessoal e individual *per se*, não possa ter uma definição axiomática, uniformizada ou fixa. Cabe apenas falar sobre suas fronteiras, seus enquadramentos e limites, tentando identificar e classificar seus possíveis contextos, para discussões referentes à relação destes com suas variantes no plano intersubjetivo, isto é, em suas manifestações socioculturais.

Assim, a privacidade se revela como nossa capacidade de gerenciar, de maneira soberana e separável, nossos diversos papeis sociais, em domínios dinâmicos e complexos onde esses papéis são vividos, animados no domínio pessoal de um mesmo indivíduo (cada um de nós). Esse processo possui um componente instintivo que, contudo, não deve ser considerado como algo inconsciente, pelo menos não completamente, pois possui um aspecto

39 O melhor exemplo é a doutrina Homeland Security dos EUA. Na página da White House pode-se acompanhar o progresso da sua aplicação: http://www.whitehouse.gov/issues/homeland-security/ (carregado em 29 de junho de 2013). O organograma da Homeland Security Research demonstra que o sistema consiste de 187 agências governamentais com competências verdadeiramente extraordinárias para efetuar qualquer e todo tipo de vigilância ou ações militares. http://www.homelandsecurityresearch.com/wp-content/uploads/2009/12/US-HLS-HLD-Structure-2010.pdf (carregado em 29 de junho de 2013).

40 Thomas Hobbes foi o primeiro filósofo da idade moderna que formulou a teoria do contrato social (na obra intitulada Leviathan de 1651). Hobbes afirma que homens, temendo o estado natural (guerra de todos contra todos), desistem de seus direitos pessoais em favor do soberano em troca da proteção e da sociedade funcionando melhor. Esta desistência de direitos é resultado da escolha racional e egoística do indivíduo que tende a conseguir a segurança máxima possível (acessível). Hobbes denomina o estado com o termo Leviatã (um monstro mítico) e indica que é impossível recuperar as liberdades individuais já transferidos, mesmo com base em um contrato social. "Hobbes: Moral and Political Philosophy", Internet Encyclopedia of Philosophy, http://www.iep.utm.edu/hobmoral/ (carregado em 29 de junho de 2013).

41 Por exemplo, no livro "Brain Sex" de Anne Moir and David Jessel, de 1989.

intuitivo, aparentemente natural e universal, o qual podemos inferir que é guiado por processos cognitivos. Definida assim, a privacidade deve ser enxergada como algo biologicamente natural, socialmente fundamental, e que merece a proteção em forma do direitos legais.

Por sua vez, a era digital trouxe avanços tecnológicos que, em contraponto a suas vantagens óbvias, criaram novos tipos de riscos e ameaças à privacidade e cujas consequências não podem ser facilmente previstas. Cabe aqui observar um fenômeno recente que corrobora tal afirmação. Nas sociedades tecnicamente mais desenvolvidas, a privacidade é protegida legalmente na esfera digital de uma maneira mais abrangente que a "privacidade tradicional" que em vários sistemas legais compreende (pelo menos) proteção física, proteção conta invasão de domicilio e proteção de correspondência. Este julgamento se baseia na estimação da quantidade e, também, complexidade das leis existentes a respeito, mesmo que a execução e a eficácia das mesmas sejam problemáticas.

Outro fenômeno curioso que merece ser mencionado, e que pode estar associado à natural dificuldade em se definir com precisão o que seja privacidade, são as tentativas e pressões para se estender o alcance de proteções legais originalmente destinadas ao indivíduo e seu reduto mais íntimo (o lar), a instituições e pessoas jurídicas. Várias discussões sobre a privacidade consideram, para isso, mais um aspeto que pode ser tido como constituinte da privacidade – o organizacional – apesar daquelas organizações já serem tuteladas, com direitos específicos, por outras áreas do ordenamento jurídico, como por exemplo os que garantem a soberania dos Estados, ou os que protegem as empresas contra espionagem industrial e outras práticas desleais.

O presente texto não se estende ao aspecto organizacional, embora esse aspecto certamente abra importante campo para pesquisas teóricas sobre privacidade. Além disso, por motivos óbvios, a presente monografia é limitada aos aspetos comunicacional e informacional da privacidade pois são esses que se referem diretamente à interação dos usuários com a rede aberta. Não obstante, vários fatores que influenciam nossa privacidade de forma virtual (tecnológica, em geral), e que têm suas origens fora dessa rede, poderão ser também sinalizados. Isso é justificado pela predominância de formatos digitais na codificação e armazenamento de dados hoje em dia, talvez pelo fato de isso torná-los mais facilmente processados, agregados, interpretados, copiados, transformados e transferidos.

Existe mais um aspecto importante que se deve considerar sobre privacidade – o mercantil. Controlar a privacidade, isto é, exercermos soberania sobre nossos papeis sociais enquanto os vivemos separadamente, é tarefa delicada por se tratar de um processo de mão dupla. O exercício de um papel social sempre envolve comunicação, a qual pressupõe troca alternada de dados (entre uma fonte e um destinatário), num contexto onde esses dados informam o destinatário sobre algo a respeito da fonte. O controle da privacidade se exerce na medida em que a fonte possa antecipar quais dos dados por ele emitidos nessa comunicação poderão ser recontextualizados pelo destinatário, via integração com metadados capturáveis noutros contextos referentes à mesma fonte, e que passam assim a informar esse destinatário também sobre outros papéis que a mesma fonte também desempenha na sociedade.

No contexto deste trabalho, podemos dizer que a sociedade da informação se caracteriza pela potencial proliferação de oportunidades onde tais recontextualizações se tornam monetizáveis (isto é, conversíveis em ganhos pecuniários). Por isso, em muitas situações os indivíduos são hoje tentados a trocar o controle da sua privacidade por certas "vantagens". Na "via de mão dupla" da privacidade, ao iniciarmos uma conversa ou permitirmos a alguém iniciá-la conosco, nós já reduzimos o controle sobre a nossa privacidade para deixar o interlocutor entrar naquele espaço que, sob o aspecto físico, corresponde a nossa área de proteção; enquanto tentamos fazer com que o outro nos permita entrar na sua.

Isso acontece em todos os níveis de interação humana, necessários ao exercício dos possíveis papéis sociais. Ao requerer crédito, por exemplo, devemos informar ao banco sobre a nossa capacidade creditícia, informação esta que é extremamente pessoal e sensível à revelação (isto é, facilmente recontextualizável para outras situações valiosas). Ao desejarmos viajar de avião, temos de nos submeter a vários procedimentos que visam a nos identificar, principalmente como fonte de ameaça a esse meio de transporte altamente sensível a riscos, procedimentos que representam invasão crescente à nossa intimidade (isto é, ao aspecto físico da nossa privacidade), tais como revistas pessoais, *scans* de raios X, biometria, etc.

Na realidade, para participarmos da sociedade, através dos papéis que nela exercemos, nós entregamos, o tempo todo, vários elementos determinantes para a nossa privacidade a outrens, sejam eles agencias estatais, empregadores, empresas comerciais ou outros indivíduos. Assim, de certo modo, a privacidade exerce na sociedade uma função semiológica equivalente à função normalmente atribuída na economia ao dinheiro. E isso acontece (ou seja, as "trocas" de controle semiológicas) muito mais frequentemente do que as trocas de caráter puramente financeiro.

Pela ausência de moeda nesse tipo de troca, podemos definir essa classe de transações, nas quais o intercâmbio é entre possibilidades de controle contextual, como uma espécie de *"barter"* – um escambo ou intercâmbio de natureza semiológica – entre um indivíduo e outras pessoas ou entidades envolvidas numa situação comunicativa. Esse tipo de troca sempre existiu, e é, sem dúvida, base para a convivência e a organização social sadias. A sanidade desse procedimento de intercâmbio semiológico advém da sua natureza (de *barter*), e não das possibilidades para monetização dos seus efeitos.

A era digital, obviamente – e de uma maneira dramática – acaba com o padrão original de separação dessas funções. Antes, o intercâmbio semiológico (ou seja, a troca – ou *barter* – de elementos de controle da privacidade dos interlocutores numa situação comunicativa) era momentâneo, e seus potenciais efeitos, instantâneos. Agora, é possível e muito fácil preservar o contexto em que se deu o intercâmbio semiológico (com a gravação de dados e metadados). Assim, elementos determinantes para a nossa privacidade podem ser analisados e combinados com outras fontes de informação, para possíveis recontextualizações. Esses elementos assim se tornam monetizáveis, e as correspondentes bases de dados, um produto evidentemente muito valioso.

O intercâmbio semiológico da privacidade, originalmente puro e estabilizador (enquanto autoajustável entre interlocutores), fica agora desbalanceado em favor dos que controlam as infraestruturas digitais de comunicação, e os consumidores de bases de dados agregáveis sob tal controle, em posições mercadológicas favoráveis à monetização dessas bases. Os indivíduos continuam trocando o controle da sua privacidade por certas "vantagens", mas para eles essas vantagens não têm, via de regra, nenhum valor monetizável.

Por causa do número crescente de usuários da rede aberta, enfrentamos uma "erosão de preços" da privacidade (assim percebida como "produto"), pois a oferta cresce muito mais rápido do que a demanda e os ofertantes não se preocupam com a natureza mercantil dessa troca (aparentemente "virtual", mas essencialmente "comercial"). Em outras palavras, os usuários vendem (mais ou menos inconscientemente) sua privacidade literalmente por nada, alavancando um novo mercado de dados – dados que poderíamos chamar de pessoalizáveis – que assim cresce sem controle, de forma distorcida (pelo efeito-rede) e, essencialmente, injusta socialmente. Os motores deste negócio são o consumerismo e uma crença universal na eficácia do marketing individualizado e o seu combustível, que são dados pessoalizáveis. Além disso, o produto "privacidade", ao contrário dos recursos naturais, é ilimitado e renovável.

Uma pesquisa de junho de 2013[42] demonstrou que 57% de consumidores querem

42 "Amdocs Survey: Consumers Will Share Personal Data… at a Price",

compartilhar ainda mais informações pessoais (do que já disponibilizaram), como sua localização, os seus cinco melhores amigos do Facebook, informações sobre os membros da sua família, em troca de vantagens financeiras ou serviço diferenciado. 54% concordam com a transferência destes dados a terceiros, sob condições "adequadas". A pesquisa, que foi global e abrangeu 3900 respondentes, aconteceu logo depois do escândalo que revelou o projeto PRISM da NSA, pelo que podemos suspeitar que os resultados seriam diferentes se a pesquisa fosse feita antes destas notícias alarmantes (as percentagens poderiam ser maiores). Esta pesquisa sinaliza que os consumidores querem trocar seus dados por vantagens medidas em dinheiro. Isso pode ser o começo de um comércio de dados pessoais no qual as pessoas físicas desempenham o papel ativo e mais justo (o que, porém, não diminui os riscos à privacidade). M. Haris da Amdocs afirma que os dados pessoais têm potencial de virar uma nova forma da moeda da indústria (*industry currency)*.[43]

3. Erosão da privacidade na rede aberta

3.1. Introdução

A perda de privacidade na época digital é um fato que não é limitado apenas aos *"netizens"*. Todos os cidadãos estão sendo afetados. Estamos cada vez mais subordinados aos sistemas de controle sobre o que fazemos e até mesmo sobre o que poderíamos fazer e pensar, e a rede aberta é apenas uma das fontes desses perigos. Na realidade, as principais funções da informatização – economia de tempo, dinheiro e outros recursos – rapidamente perdem importância (sendo esta presumida, embora falsa[44]) e no lugar delas surge a onipresente *função controladora*. A informatização contemporânea já não tem como objetivo acelerar a troca de dados, mas sim controlar quão corretamente se dá essa troca, conforme padrões comerciais e políticos. A informatização na vida humana, a partir das últimas décadas do século XX, deslocou para segundo plano a função da informatização que era primordial, a de facilitar a realização de cálculos, que poderia enriquecer o nosso conhecimento. Hoje, lidamos mais com problemas de separação de processos de cálculo do que com aqueles relacionados à correção matemática interna deles. Este fato é acompanhado por outro fenômeno muito esquisito e perigoso: a crença na corretude absoluta dos processos digitais que se manifesta pelo "otimismo digital geral" (ou tecno-triunfalismo, que o prof. Rezende batizou de "Seita do sando byte"[45]). A partir da metade do século XX, quase em todo o mundo, presenciamos uma onda de informatização dos processos relativos à burocracia estatal e do mundo de negócios, o de grandes corporações em particular. Esta nova burocracia digital é proclamada como algo por definição melhor, mas, no fundo, isso é nada mais que um mito. A burocracia é burocracia, tanto faz quais ferramentas ela utiliza para se manter. Pensando bem, será que com o advento da tecnologia digital a burocracia diminuiu globalmente? A burocracia digital é simplesmente menos humana, ou desumana mesmo. Garfinkel indica que:

Os governos e o mundo de negócios começaram a adquirir computadores em massa na segunda metade do século XX, substituindo bilhões de arquivos de papel com sistemas

---

http://www.amdocs.com/News/Pages/amdocs-personal-data-consumer-survey.aspx (carregado em 5 de julho de 2013).

43 Michal Harris, "Looking Through the PRISM: Three Customer Data Lessons", http://blogs.amdocs.com/insightfuel/2013/06/20/looking-through-the-prism-three-customer-data-lessons/ (carregado em 5 de julho de 2013).

44 Charles Jonsher, no livro "Wired Life, Who Are We in the Digital Age?" de 1999, dedicou o capítulo 7, intitulado "Em busca de resultados. Computadores versus crescimento econômico", ao misterioso fiasco das tecnologias de informação na produção de efeitos positivos na economia (o assim chamado "paradoxo da eficiência"). Os computadores, softwares, trabalho de peritos, comunicação, etc. são todos muito caros e, grosso modo, não demonstraram nenhuma economia de recursos financeiros, na sua aplicação. O que realmente mudou na época digital é o caráter do nosso trabalho e os modelos de negócios.

45 Pedro A D Rezende, "A Seita do Santo Byte", http://www.cic.unb.br/~rezende/trabs/azeredo.htm

eletrônicos de processamento de dados. Hoje, os humanos estão, frequentemente, ausentes nos processos digitais decisionais. Em resultado, criamos um mundo no qual o menor erro de um funcionário pode ter efeitos devastadores na vida de uma pessoa. Este é o mundo em que os computadores são presumidos de estarem corretos e as pessoas são presumidas de estarem erradas[46]. [tradução do autor].

Por enquanto, são os humanos que criam os softwares (pelo menos, na parte grande) para esta nova burocracia digital e são eles mesmos que são responsáveis pelos erros contidos neles. Mas na realidade, os procedimentos elaborados por cima das regras burocráticas são percebidas como não falháveis. Computadores parecem ser mais corretos do que humanos. Observamos isso quase cada dia ao estarmos atendidos pelos funcionários de agências estatais, bancos, lojas, postos de gasolina, etc. Quantas vezes, ao tentar resolver um assunto simples, ouvimos de um funcionário munido de computador algo do tipo: "o sistema não permite...". A propósito, os funcionários dependentes da tecnologia digital, frequentemente, nem sabem utilizar o computador de uma maneira adequada. Para eles, o computador não é uma ferramenta que deve facilitar o seu trabalho, mas um elo no controle de sua corretude como empregados (*chilling effect*).

As ameaças à privacidade de usuários na rede global surgem por causa de uma combinação dinâmica de vários fatores: econômicos, técnicos e tecnológicos, psicológicos e outros (como relacionados à moda, por exemplo), falta ou inadequação da lei ou sua aplicação atrasada. Dentre esses fatores, devemos apontar, antes de tudo, a possibilidade e facilidade de obter dados pessoais e a presença de sujeitos interessados em obter esses dados. Neste texto, definimos seis categorias desses sujeitos: entidades comerciais, entidades estatais, empregadores, provedores de internet, criminosos e pessoas físicas comuns, entre elas, infelizmente, nossos entes mais próximos (parentes, cônjuges, filhos e amigos).

Além dos motivos para a coleta de dados sobre os usuários da rede, podemos indicar ainda um outro fator de categorização de possíveis invasores, que é o alcance ou a escala dessa coleta. As pessoas físicas, nossos parentes e amigos (em particular ex-cônjuges, ex-amigos, ex-namorados/namoradas) podem coletar dados sobre nós, abrangendo a escala de uma única pessoa (mas podem publicá-los em sites sociais, o que os torna, efetivamente, globais). As empresas empregadoras coletam dados sobre os seus empregados, isto é, dentro da escala que corresponde ao número de empregados que possui (podendo esse número ser muito elevado, no caso de grandes empresas nacionais ou transnacionais, por exemplo). As empresas provedoras de internet podem coletar dados sobre seus clientes, isto é, em escala local, regional ou nacional. As empresas comerciais típicas podem coletar dados sobre os usuários que visitam seus sites, fornecedores e parceiros, que podem dizer respeito a uma escala local a transnacional. Os órgãos estatais podem coletar dados e observar os usuários da rede em escala nacional e até mesmo transnacional. Finalmente, as empresas donas de motores de busca ou de serviços pela rede efetuam essa coleta em escala global. Cabe ressaltar que alguns órgãos estatais são capazes de monitorar toda a rede (ou quase toda), no nível mais inferior da comunicação, relativamente ao restante das entidades, forçando os donos ou administradores da infraestrutura a revelar e/ou gravar o fluxo de pacotes atravessando a rede, ou farejando a transmissão de sinais eletromagnéticos, ou forçando as entidades comerciais e outras a revelarem os dados por elas acumulados.

Devemos enxergar que a interação com a rede pressupõe uma possibilidade, e até mesmo necessidade, de manipulação de "personalidades digitais" dos seus membros, que são apresentadas ao público. Todos os sujeitos presentes na rede tendem a idealizar sua imagem, não importa se se trata de pessoa física ou de entidade coletiva, comercial, em particular. Para fazer isso, todos têm que, de certo modo, manipular o público ou até mesmo mentir e, por outro lado, aceitar manipulações e mentiras. Aqui, não condenamos moralmente a mentira em

46 Simson Garfinkel, "Database Nation, The Death of Privacy in the 21st Century", p. 12.

si. Ela pode ser "branca" ou efetivamente não perigosa. Mensagens de propaganda, via de regra, contêm comunicados exagerados, embora cuidadosamente projetados para manipular as mentes dos destinatários, e isso parece ser amplamente aceitável. Mas, na realidade, essas atividades disseminam semiverdades ou mesmo não-verdades. Os nossos perfis digitais também não precisam estar corretos e nem atuais, como, aliás, qualquer informação publicada na rede aberta não precisa. É essencial enxergar que, na época digital, uma semiverdade ou uma mentira em formato digital pode ser, e até mesmo é, analisada automaticamente para obtenção, assim, de uma medida numérica. Partindo dessa observação, logo vemos que toda a interação dos humanos entre si, intermediada pelo plano da computação, pode se tornar uma mera tarefa informática que seja um jogo de semiverdades ou mentiras numericamente codificadas, direcionadas à manipulação do recebedor, privada de quaisquer emoções, que são laços comunitários primordiais. Este jogo de falsificar a sua própria imagem para manipular o público de uma maneira completamente desalmada torna a rede aberta um palco em que, por definição, espalha-se narcisismo em escala inédita. Isso constitui potencialmente uma injúria a indivíduos e entidades, muito mais dolorosa do que a sinalizada por Warren e Brandeis no fim do século XIX e muito mais abrangente, já que não afeta só os astros cobiçados pela mídia, mas sim qualquer um que deixe os traços de sua presença na rede aberta. De certo modo, na rede podemos todos nos tornar "astros" (antes de mais nada no sentido de ser alvos de ataques), e a mídia, agências estatais ou quem quer que seja podem acessar quaisquer dados sobre nós em milissegundos (e, também, ter acesso a nós mesmos: telefonando, enviando e-mails, localizando-nos geograficamente, entre outras formas de localização). Realmente, a internet parece ser uma apoteose do mito sobre Narciso e este mito, a propósito, não é positivo, como tal. A internet tornou-se um espelho das sociedades modernas dominadas pelo consumerismo que se baseia fortemente na manipulação do público.

Alguns autores dos textos sobre a privacidade afirmam que a tecnologia em si não constitui uma ameaça para nós – o perigo sempre vem de pessoas maldosas em cujas mãos o controle dela se encontra e que a utilizam para fins ou por meios escusos. Exemplificando esta tese, Marcela e Stucki convocam o controle de armas: *Guns don't kill people; people kill people*.[47] Conforme os autores, é a nossa natureza humana que gera riscos, perigos e ataques contra a nossa condição e/ou existência como humanos. Esta tese, porém, não precisa ser completa, pois é colocada em um nível de abstração não bem definido. Ela sugere que os humanos e a tecnologia são entes separáveis, ou que a tecnologia é algo neutro. Garfinkel aponta que a ideia de que a tecnologia é neutra é muito confortável, embora errada:
A história é cheia de efeitos desumanizadores da tecnologia. Embora seja possível utilizar a tecnologia para proteger ou melhorar a privacidade, a tendência nos avanços tecnológicos é de se fazer o contrário. É mais difícil e, frequentemente, mais caro construir dispositivos ou elaborar serviços que protejam a privacidade, do que os que a destruam[48] [tradução do autor].

A tecnologia é criada e modificada por humanos e em seguida influencia a vida deles. O problema é que nunca podemos ter certeza absoluta de como ela será utilizada e qual será o seu impacto na nossa vida. Os humanos tendem a superestimar o impacto a curto prazo das tecnologias novas e subestimar os seus efeitos a longo prazo.

Existe um fenômeno, frequentemente observável na área de educação, da deslocação da percepção da fonte de ataques contra os usuários comuns da rede aberta. Os usuários leigos do computador, os novatos, entre eles as pessoas de idade, às vezes antropomorfizam o computador em seus primeiros contatos com ele. Eles parecem tratá-lo como um ser vivo, seu potencial amigo, alguém interessante, atraente, em que se depositam confiança e esperança. A

47 Albert J. Marcela Jr., Carol Stucki, "Privacy Handbook, Guidelines, Exposures, Policy Implementation, and International Issues", p. 11.

48 Garfinkel Simson, "Database Nation, The Death of Privacy in the 21st Century", p. 258.

mesma dedicação ingênua pode-se observar na interação inicial deles com a internet, que lhes parece infinita, oferecendo mais do que se pode imaginar e lembrar, presumidamente boa e cheia de possíveis vantagens e futuros amigos. A esfera da computação, cujo papel é comumente incompreensível, engana sentidos e instintos humanos, inclusive o de privacidade. Sendo ofendidos de surpresa pela interação com a tecnologia digital, alguns usuários culpam-na, ou até mesmo o computador, e não os humanos que a utilizam como uma ferramenta de manipulação para ganhar poder ou dinheiro. A perda de privacidade, bem como outros fenômenos que têm lugar na época digital, tem sua origem na nossa natureza humana que, por um lado, busca reclusão e paz e, por outro, tende a perturbar a reclusão e paz dos outros. A esfera intermediadora da computação, bem como a ingenuidade dos usuários, às vezes promove a transferência artificial da responsabilidade pelas violações de nossa privacidade e por outros problemas da época digital dos humanos à tecnologia.

Recapitulando, os fundamentos da erosão da privacidade na época digital não são nem puramente "digitais", nem puramente "humanos", são uma conjugação da tecnologia e dos fatores humanos, que junto geram uma "mistura explosiva". Garfinkel faz uma observação interessante em relação à nossa natureza humana:

Humanos são colecionadores inatos. Psicologicamente, é mais fácil ficar com algo do que jogá-lo fora. Isso é ainda mais verdadeiro em relação aos dados. Ninguém realmente sente-se confortável deletando sua correspondência de trabalho ou apagando registros antigos – nunca se sabe quando algo vai ser útil. A tecnologia avançando possibilita realizar o sonho coletivo de nunca ter que jogar nada, ou pelo menos nunca ter que jogar fora nenhuma informação [tradução do autor][49].

Esta afirmação vale tanto para usuários, como colecionadores e consumidores de seus dados e, na verdade, qualquer sujeito ou entidade presente na rede aberta. Todos colecionam dados e não os deletam. Então, os dados sobre nós, que colocamos em volumes enormes na rede aberta, com altíssima probabilidade nunca serão deletados e em algum momento poderão ser utilizados por motivos para nós indesejáveis.

As questões da proteção da privacidade são sempre sopesadas contra os interesses e/ou padrões éticos e morais da sociedade como um todo. Neste contexto, a segurança pública é algo particular. Um acontecimento – os ataques ao World Trade Center e a outros prédios nos Estados Unidos em 2001, que resultaram na morte de milhares de pessoas inocentes – causou um radical desequilíbrio entre esses dois valores sociais importantes[50]. Os efeitos de longo prazo não se limitam aos Estados Unidos. O mundo inteiro sofreu por causa desses ataques, pois está cada vez mais interdependente sob todos os possíveis pontos de vista. Como resultado disso, muitas pessoas, em várias partes do globo, passaram a concordar com a limitação de sua própria privacidade e até mesmo de sua liberdade e outros valores referentes à cidadania, em troca de uma suposta *segurança maior*.

Mas como se mede a segurança? Como podemos saber se ela está realmente maior em relação ao que era? Parece que, para os cidadãos comuns, o aumento da segurança não é objetivamente nem diretamente perceptível, pois para isso seriam necessários, no mínimo, tempo e paciência (as estatísticas deste tipo, pelo menos por enquanto, ainda não são instantâneas). Para esses cidadãos, uma medida do eventual aumento de sua segurança acaba sendo a perda da liberdade civil, pois esta é visível quase em cada momento, em cada lugar. Mas eles consentem em perder tal liberdade por indução das autoridades, que se aproveitam do seu medo e desespero, muitas vezes insuflado por propaganda oficial. Esses fatos geram preocupações sociais e morais seriíssimas. Zelando pela segurança, ou simplesmente

49 Ibid. p. 75.

50 Este evento, na verdade, é um dos muitos fatores que têm consequências sociais graves, no que diz respeito à privacidade e liberdades civis. Nos EUA, muitos cientistas e jornalistas apontam, entre outros: Guerra Contra Narcóticos (proclamada em 1971 pelo presidente Nixon), Guerra Contra Pornografia e, atualmente, Guerra Global Contra Terrorismo.

afirmando zelar, ato este que não é verificável e nem visível por seus efeitos a curto prazo, as autoridades obtêm a permissão de limitar a privacidade e até liberdade dos cidadãos. Mas essa circunstância dá a elas ainda mais poder (mais do que seria objetivamente necessário), e esse excesso de poder pode ser utilizado não apenas para aumentar a segurança dos cidadãos contra os supostos riscos, mas também para fortalecer o controle sobre a sociedade e, na época digital, sobre cada um de seus membros separadamente, já que estes podem ser – e são – acessíveis individualmente por meio da rede aberta e de muitas outras tecnologias, quase que instantemente.

Essa técnica de "pegar carona" em algum acontecimento que represente perigo para a sociedade, ou para outro grupo de indivíduos, visando obter ou aumentar o controle sobre seus membros é bastante comum e frequentemente envolve um quê de "caça às bruxas", isto é, compromete, ostraciza, bane ou elimina eventuais oponentes. Esse modo de atuação pode até ser tido como "natural", quando advém da religião. Quem não deseja maior segurança após o 11 de setembro? – só mesmo um terrorista. Quem não deseja que se persigam os pedófilos? – só um pedófilo. Quem não acredita em algo que é amplamente aceito? – só um inimigo da sociedade. Desse modo, gera-se histeria no povo, cala-se a oposição, mata-se a coragem civil e obtém-se permissão para maior controle sobre todos. Logo, são ouvidas declarações de que a melhor maneira de detectar terroristas, pedófilos e outros criminosos, bem como aqueles que são de alguma forma diferentes, é vigiando toda a internet (ou outros meios de comunicação). Mas, desse modo, pode-se perseguir também os oponentes políticos ou obter vantagens de qualquer outro tipo, limitar as liberdades civis, minar os princípios da democracia e abrir caminho para várias distorções dos sistemas políticos estabelecidos e comumente percebidos como sadios.

Os exemplos supramencionados a respeito da "técnica de pegar carona" podem até soar extremos, mas pode-se facilmente observar variações dessa manipulação em situações mais comuns, como por exemplo, no mundo da tecnologia digital.

Os produtores de softwares e hardwares, bem como os prestadores de vários serviços na rede tendem a forçar os usuários a se cadastrar, revelar sua identidade e dados demográficos, providenciar o acesso aos conteúdos programáticos de seus computadores (telefones, tablets) e entregar os direitos de utilização de conteúdos não programáticos (como e-mails, documentos, imagens e multimídia, que os usuários colocam em nuvem), permitir sua localização geográfica, e tudo isso é apresentado como sendo exclusivamente dedicado ao melhor atendimento ao cliente, à qualidade de produtos e serviços, segurança, entre outros. Aos usuários, são apresentados vários tipos de ameaça, como: spam, furto de identidade, perda de dados ou de acesso a serviços, entre outras. Se eles não concordarem com tais condições, não poderão utilizar mais os serviços e perderão dados e/ou o acesso a eles. No fundo, isso nada mais é do que uma chantagem (comercial, mas não apenas isso).

Será que é mesmo indispensável, para um produtor de sistemas operacionais ou hardware ou qualquer outra tecnologia, saber onde eu moro ou me encontro, qual é a minha idade e profissão, quantos filhos tenho e qual é o meu salário? Como esse produtor vai aumentar a qualidade (relativa à segurança, por exemplo) do seu sistema operacional ou seu dispositivo com o uso dos meus dados pessoais? São eles exatamente o que estava faltando para tornar esse sistema ou aparelho mais bem protegido e mais útil? Temos aqui um exemplo muito simples de como os monopolistas utilizam sua posição para fortalecê-la ainda mais, manipulando e/ou chantageando seus clientes, invocando riscos reais ou criando ilusórios e transferindo a responsabilidade por suas faltas a uma multidão despersonalizada de inimigos.

Mas, sem dúvida, para se aproveitarem da presença no ciberespaço, os usuários têm que informar sobre si quando entram nele. Fazendo compras na rede, via de regra precisamos de cartão de crédito que, a propósito, já nos identifica plenamente e informa de quem, onde e por que preço compramos (os donos de lojas sabem disso, podem vender esta informação ou

podem ser forçados a revelá-la). A participação em redes sociais não faz sentido se um usuário permanece anônimo[51]. Em várias situações, sem a redução das nossas expectativas de privacidade, não podemos utilizar a rede de uma maneira útil e cômoda. Um dos problemas é que os usuários revelam sistematicamente muita informação sobre si, inclusive quando isso é desnecessário. Frequentemente, os usuários comuns revelam seus *dados verdadeiros*, pois muitos de nós fomos criados em ambientes socioculturais (inclusive os religiosos) nos quais a mentira é condenável perante os portadores da "verdade absoluta" (parentes, líderes de comunidades religiosas, etc.). Eles fazem isso por falta de cuidado, desconhecimento ou falta de compreensão dos riscos, negligência, vontade humana de se socializar e, também, em decorrência de manipulação psicológica e até mesmo de chantagem; afinal, os usuários podem acabar sendo forçados a identificar-se sob pressão de não poderem utilizar serviços ou de perderem dados já acumulados[52]. Do outro lado, existem sujeitos que sabem fazer negócio adquirindo, processando e vendendo esses dados e que sabem induzir ou forçar os usuários a revelá-los.

Não há mais dúvidas: o comércio de dados pessoais é um negócio enorme e lucrativo, mas as estimativas de lucratividade dele não são fáceis de traçar, como demonstra, por exemplo, o relatório da OECD de 2013[53]. Como qualquer atividade comercial sem controle legislativo e administrativo eficaz, esse comércio ultrapassa todos os limites possíveis, em particular os morais e éticos tradicionais, que não nos servem mais, e os novos limites ainda estão "engatinhando". A vigilância de pessoas no mundo real é perseguida pela lei de todos os países do mundo civilizado – a menos que seja feita pelas agências estatais, que não revelam suas ações e seus motivos voluntariamente. Espreitar pessoas presumivelmente inocentes é imoral e condenável. Por que fazer o mesmo com os usuários da rede aberta não deveria ser considerado igualmente imoral?

Recapitulando, do ponto de vista técnico, as ameaças à privacidade de um usuário da rede vêm do fato de existirem possibilidades de se obter acesso aos dados desse usuário ou a respeito dele que ele guarda no seu ou em outro computador (em nuvem), transmite e recebe, de se processar esses dados, agregá-los com outros e utilizar com outra intenção, diferente da que foi (se é que realmente foi) informada ao usuário, sem o consentimento ou conhecimento deste. Esses dados podem, em seguida, servir para a geração de um perfil digital desse usuário, a comercialização desse perfil e o tratamento do usuário como alvo de propaganda individualizada ou manutenção deste perfil para qualquer outro tipo aplicação. Em particular, esses dados podem servir para controlar a postura desse usuário como cidadão, empregado ou até mesmo cônjuge, colega ou simplesmente ser humano. Eles podem facilitar a observação ou vigilância do usuário, inclusive no que diz respeito à sua condição financeira, estado de saúde, interesses, compras, simpatias políticas, religião, orientação sexual, contatos com

51 Mesmo assim, devemos pensar nas situações em que isso poderia servir para observação, infiltração e mesmo ataque aos usuários do serviço, o que não é de forma alguma incomum. Os serviços das redes sociais são excessivamente vasculhados pelas autoridades de segurança pública, por empregadores e criminosos.

52 A Microsoft anunciou uma alteração da política de acesso pelos usuários aos serviços de e-mail (hotmail), bing, office.com e outros, válida a partir de 19 de setembro de 2012, com antecedência de apenas cinco dias. Os usuários têm de se subordinar às novas regras sem nenhuma possibilidade de negociação. Eles só têm a opção de desistir desses serviços e ferramentas e perder seus dados. As novas regras demandam identificação, consentimento de utilização de técnicas de localização física, permissão para utilizar conteúdos multimídia e verificar softwares no computador local, entre outras ações. Mas a empresa declara que isso tudo é exclusivamente para o bem dos usuários... http://www.dailytech.com/EU+Investigates+Microsoft+for+Policy+Changes+in+Hotmail+Bing/article29462.htm. As mesmas alterações abruptas acontecem periodicamente em outros serviços como Facebook, Google, etc., sempre causando protestos que logo se calam e a situação "normaliza-se" em favor dos provedores.

53 OECD (2013), "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value", OECD Digital Economy Papers, No. 220, OECD Publishing. http://dx.doi.org/10.1787/5k486qtxldmq-en (carregado em 18 de junho de 2013).

outras pessoas (incluindo membros da família), propriedades, planos de vida, localização geográfica, entre outros. Sem dúvida, os dados pessoais podem servir também para perseguição política, religiosa, sexual ou para outros fins. Finalmente, esses dados podem ser utilizados para cometer crimes como, por exemplo: invadir a conta bancária do usuário ou outro serviço que exige identificação ("roubo" de identidade) ou comprometer e lesar o usuário por meio da divulgação de informações pessoais ou chantageá-lo com tal ameaça.

Neste ponto, devemos fazer uma observação importante. Os dados do computador local podem ser acessados por alguém que tenha acesso físico a ele. Neste caso, todas as regras de negócios, a lei ou as técnicas sofisticadas de ataques não são necessárias, pois alguém que tem acesso ao computador (o administrador da rede local em um café ou em uma empresa, um membro da nossa família, etc.) pode simplesmente copiar qualquer informação pertencente ao usuário. *Na época digital, o computador pessoal tornou-se de fato algo extremamente pessoal.* Na maioria dos casos, os computadores pessoais de usuários comuns armazenam as informações mais íntimas sobre os seus donos. Frequentemente, na mídia, aparecem notícias sobre a detenção de pessoas suspeitas de crimes. Em todos esses casos, a polícia ou outras entidades de segurança buscam apreender também computadores, telefones, dispositivos de memória, etc., pois estes podem revelar detalhes mais íntimos relacionados à vida dos suspeitos.

A acessibilidade e visibilidade dos dados pessoais e de qualquer outro tipo de dado sobre uma pessoa (localização, comunicação, compras, interesses, simpatias, pensamentos, entre outros) é efetivamente equivalente à observação constante dela em sua casa, com sua família, durante uma viagem, no contato com os outros, ou, melhor dizendo, no exercício de seus papéis sociais, sendo eles reais, declarados ou impostos. De certo modo, isso é semelhante a possuir um leitor de mente embutido na cabeça que transfere sua visão, audição, fala e qualquer emoção ou ação a outros seres humanos, identificados ou não.

Como já mencionamos, a informação, ou, mais precisamente, a posse dela em contextualizações vantajosas, equivale ao poder. A possibilidade de manipular a informação equivale à manipulação do poder. A manipulação do poder direciona-se sempre ao seu fortalecimento, que leva ao seu excesso, e nunca desiste do que já conseguiu conquistar (os pensamentos de Hobbes, do século XVII, permanecem brilhantemente atuais na época digital). É este fato tão simples que gera tantas preocupações por parte das pessoas conscientes e capazes de enxergar os riscos. Infelizmente, a maior parte dos cidadãos, usuários da rede em particular, não é capaz, desiste ou não os quer enxergar.

3.2. Deficiências da arquitetura da rede aberta

Pela arquitetura, compreendemos aqui os elementos em um nível de abstração maior em relação àquele da mera infraestrutura física da rede aberta, embora esta também seja importante. Descreveremos o modelo de comunicação e seus protocolos, elos intermediários, linguagens para construir conteúdos de páginas e softwares, tais como navegadores.

Em um roteiro mais comum de interação pela rede, um usuário físico acessa um servidor (http, correio, entre outros) por meio da rede aberta. Para fazer isso, ele precisa possuir um número IP e conseguir o número IP do servidor desejado mediante o uso do serviço DNS. Estando conectados por meio da infraestrutura da rede, o computador do usuário e o computador-servidor podem transmitir dados entre si. Existem muitas famílias de protocolos de comunicação pela rede aberta, mas nos limitamo aqui às situações mais comuns em que o usuário físico carrega uma página HTML pelo protocolo http (ou https) ou acessa o correio eletrônico mediante o uso de protocolos de e-mail (SMTP, POP ou IMAP).

3.2.1. Protocolo http, https e linguagem HTML

A construção da linguagem utilizada para a criação de páginas WWW – o HTML –

bem como a especificação do protocolo http para a transferência destas (elaborado em cima dos protocolos TCP e IP), modelo de transmissão na rede aberta, e a construção dos navegadores, são todos altamente problemáticos.

O HTML, como também as outras linguagens de marcação, tem um formato de texto plano. Isso o torna de fácil criação, leitura e rápido transporte pela rede, evitando programas de antivírus. As requisições de http são também formuladas em texto plano, e a comunicação por http, em roteiros mais comuns, revela quem e com quem se comunica. Esses fatos constituem grandes vantagens da rede aberta, mas, ao mesmo tempo, também suas grandes fraquezas. A comunicação na rede aberta pode ser facilmente interceptada e, quando em formato textual, lida pelas pessoas. Sem pesquisa mais profunda sobre esse aspecto, basta dizer que os estudantes de matérias como "Transmissão de Dados" ou "Redes de Computadores", oferecidas pelos departamentos de ciência da computação no mundo todo, aprendem a fazer isso em suas aulas utilizando ferramentas gratuitas, como o programa *WireShark*, por exemplo. O protocolo http não foi projetado para garantir a segurança dos usuários, mas sim para garantir eficiência de transmissão (no que diz respeito à velocidade e detecção de erros).

Logo após seu surgimento, ficou claro que a transmissão pelo http não era adequada a todas as formas de interação com a rede, como às transações comerciais, operações bancárias, entre outras. Surgiu a necessidade de criptografar as transmissões sensíveis à revelação e foi elaborado o protocolo https – uma versão criptografada do http aliada a várias outras tecnologias destinadas ao mesmo fim.

3.2.2. Acessibilidade de endereço IP e de outros parâmetros

A própria visibilidade do endereço IP na comunicação pelo http já é problemática. O servidor http recebe essa informação logo no início da comunicação com o computador-cliente. Ele pode verificar esse endereço na rede, cruzar as requisições que chegam e buscar outras informações para aumentar o seu "conhecimento" a respeito desse endereço e do computador com o qual se iniciou a comunicação. Tendo um endereço URL, o IP pode ser encontrado utilizando o serviço DNS (descrito adiante).

O IP pode ser fixo ou concedido temporariamente. No primeiro caso, ele pode facilmente identificar o computador do usuário e até mesmo o próprio usuário. No segundo caso, ele pode fazer o mesmo se o tempo de concessão for suficientemente longo, e isso acontece, por exemplo, no caso de redes de banda larga oferecidas pelos provedores de TV a cabo. Além disso, a distribuição de endereços IP permite identificar o lugar geográfico onde residem os computadores portadores desses endereços. Essas circunstâncias resultam em tratamento do endereço IP como um dado pessoal, pelo menos em certas condições, como os cookies, descritos em seguida.

O IP é uma "etiqueta numérica", inicialmente projetada para ter quatro bytes (IP4), que identifica computadores e redes (sub-redes) na internet (sendo, no fundo, uma "rede de redes"). O crescimento rápido da rede aberta logo esgotará o acervo de endereços IP4 e, por isso, já existe um padrão IP6 (de seis bytes). Com ele, será possível conectar à rede aberta novas sub-redes e vários novos tipos de dispositivos que continuam a surgir: tablets, smartphones e até mesmo aparelhos domésticos e microssensores (smart dust). Em teoria, surgirá uma rede onde os hosts serão altamente heterogêneos, sendo, entretanto, capazes de se comunicar e se reconhecer, mesmo sem o conhecimento nem a permissão de seus donos.

Além do IP, as placas de rede (ou outros elementos equivalentes), embutidos em nossos dispositivos digitais, possuem um endereço MAC (Média Access Control), que os identifica de maneira muito mais efetiva (eles em teoria são únicos na escala global), especialmente em redes locais. Quando utilizamos roteadores, a rede externa vê o MAC do roteador e não vê os endereços IP e MAC dos dispositivos na rede local, o que é bom do

ponto de vista da proteção de privacidade e da segurança.

Existem mais modalidades de potencial reconhecimento do usuário, por exemplo os parâmetros de navegador como User Agent (nome de código do navegador) junto com os dados sobre o sistema operacional, lista de fontes instalados, etc. Estas técnicas receberam o nome de *browser fingerprinting*. O projeto da Electronic Frontier Foundation, chamado Panopticlick, permite participar na pequisa da efetividade do *browser fingerprinting* e verificar a frequência com a qual a combinação dos parâmetros de navegador aparecem na rede aberta[54].

Resumindo, a acessibilidade do IP e de vários outros parâmetros faz com que a descoberta de quem e com quem se comunica seja fácil e torna possível localizar fisicamente os usuários. Logo, a universalização da internet pode criar uma infraestrutura heterogênea e transparente que opera sem a necessidade de interação ou controle humano. Sem dúvida, não se pode esperar que essa perspectiva reduza os já grandes riscos à privacidade.

3.2.3. DNS

Via de regra, os usuários comuns nem sabem da existência de endereços IP na rede. Eles só enxergam os endereços URL, que, a propósito, foram criados para fazer o "etiquetamento" de hosts (servidores http e outros recursos) mais legível às pessoas. Mas os computadores na rede comunicam-se pelos protocolos de nível inferior, que utiliza os IPs. Para traduzir os URLs (também chamados de nomes mnemônicos) para seus respectivos IPs, precisa-se de mais um serviço – o DNS (Domain Name System ou Sistema de Nomes de Domínios). O DNS, em sua arquitetura, é um banco de dados hierárquico e distribuído. Ele é capaz de fazer também a tradução reversa, isto é, do IP ao nome correspondente (o DNS reverso). Em roteiros mais comuns, o DNS funciona como um elo lógico intermediário na comunicação entre o computador do usuário e o servidor identificado pelo nome mnemônico. Quando o usuário escolhe um endereço URL (digitando-o ou clicando no hiperlink), o navegador recorta a parte dele que se refere ao nome do domínio no qual reside o recurso requisitado (arquivo html, css, script externo, imagem, entre outros) e o envia à porta 53 do servidor DNS, cujo endereço está configurado na interface de rede do computador do usuário. Esse servidor encontra o nome do domínio buscando na sua lista de nomes/endereços. No caso de não conseguir fazer isso, ele pode reenviar o nome para outros servidores DNS. Se eles falharem em decifrar o nome, o usuário recebe uma mensagem de erro falando a respeito do domínio desconhecido. Quando o nome é decifrado com sucesso, o navegador recebe o endereço IP do servidor http e inicia a comunicação com ele, requisitando os recursos a serem carregados no computador do usuário.

A ideia do DNS, como de vários outros elementos arquitetônicos da rede, é tão boa quanto perigosa. Antes de tudo, fazendo requisições DNS, já se revela o interesse do usuário (o domínio a ser acessado) e o IP do seu computador. Os servidores DNS podem efetuar várias outras operações além de decifrar nomes, como memorizar os endereços IP dos computadores e os nomes de domínios por eles solicitados, cruzar essas informações com outros bancos de dados e permitir a criação de perfis de navegação de indivíduos.

O DNS desempenha um papel fundamental na arquitetura da rede aberta e igualmente fundamental na segurança de comunicações. Os serviços de DNS e DNS reverso são públicos e permitem a decifração de nomes e IPs em milissegundos. Isso é muito bom, mas pode servir também para encontrar e até mesmo falsificar informações sobre os hosts por motivos escusos. A defesa contra esse tipo de ataque, do ponto de vista do usuário comum, é praticamente nula. Ele depende plenamente da correta configuração do servidor de DNS ao qual ele se conecta e que, na maioria dos casos, é automaticamente atribuído à interface de

54 Panopticlick. How Unique – and trackable – is your browser, https://panopticlick.eff.org/ (o carregado em 18 de junho de 2013).

rede do seu computador pelo seu provedor de internet. Surge aqui uma dependência da privacidade dos usuários da efetividade técnica do provedor de internet. Os problemas nesta área são bastante comuns – os servidores de DNS no Brasil foram alvo de um enorme ataque em 2011[55].

Uma observação, no que diz respeito a DNS no contexto da privacidade, é que ele pode, por definição, servir para perfilamento de usuários de maneira não menos eficaz do que cookies, web bugs e outras técnicas e aqui os usuários não tem uma opção de "opt-out"[56].

3.2.4. Classificação das ameaças segundo a sua origem arquitetônica

A análise dos elementos de arquitetura supramencionados leva-nos a uma classificação das ameaças à privacidade na rede aberta de acordo com a sua origem arquitetônica, a partir do ponto de vista de um usuário comum. As primeiras ameaças estão nas proximidades do usuário. Depois vêm aquelas relativas ao canal de comunicação que transporta mensagens. Finalmente, existem as ameaças do servidor, que fornece os conteúdos requisitados pelo usuário. Aqui, o http, como os protocolos de e-mail e outros não criptografados, são efetivamente equivalentes (no sentido dos possíveis riscos que podem trazer), pois pode-se detectar quem e com quem se comunica e o que se transmite.

Dado o tema da presente monografia, enfatizamos que falamos aqui sobre as ameaças na interação do usuário com a rede aberta e não sobre todas as ameaças à sua privacidade que possam surgir em decorrência do uso do computador. Afinal, se alguém, órgãos de segurança ou criminosos desesperados, realmente quiser obter os dados do nosso computador, eles poderão simplesmente nos algemar ou abrir com um pé-de-cabra a porta da nossa casa e apreender o nosso laptop.

Assim, a proteção da nossa privacidade digital começa pela proteção física de nós mesmos como pessoa (nossas crianças) e de nossas casas e, só depois, dos nossos dispositivos, tais como computadores, laptops, palmtops, tablets, discos rígidos, pendrives, celulares, smartphones, entre outros. Cabe ressaltar que, em qualquer sistema de informação (isto é, sistema que integra sistemas informáticos e organizações humanas), o fator humano sempre é o mais fraco. O já mencionado Kevin Mitnick, um dos hackers mais famosos do mundo e hoje especialista em segurança de computadores, afirma que técnicas de engenharia social são mais importantes do que conhecimento técnico quando se quer obter acesso a computadores e dados[57].

Voltando à utilização da rede aberta, as ameaças nas proximidades do usuário em sua interação com ela estão ligadas à navegação, em particular à acessibilidade ao endereço URL no qual o usuário navega, digitando-o na barra de endereços do navegador ou clicando em um hiperlink ou atalho previamente gravado (bookmark). Essa informação sobre o que o usuário gostaria de ver já tem valor para quem sabe utilizá-la, em particular, um valor comercial, que pode transformá-la em mercadoria. Poucos usuários sabem disso, muitos não prestam atenção. Essa informação textual pode ser facilmente lida não só pela página de busca, por exemplo, mas também pelo provedor de acesso à internet (ISP), pelo administrador da rede local ou intranet, pelos empregadores ou outras pessoas que tenham acesso ao computador do usuário e/ou à infraestrutura de comunicação. Essas pessoas podem verificar o histórico de navegação e buscar arquivos no cache do navegador, incluindo cookies. Isso é particularmente perigoso quando se utilizam computadores públicos ou compartilhados e redes ad-hoc (as redes wi-fi

55 Fabio Assolini de Kaspersky Lab Expert, artigo "Massive DNS poisoning attacks in Brazil", de 7 de novembro de 2011, http://www.securelist.com/en/blog/208193214/ (o carregado em 23 de junho de 2013).

56 The DNS Operations, Analysis, and Research Center (DNS-OARC), a presentação da Karsten Nohl da University of Virginia de 2008 https://www.dns-oarc.net/files/dnsops-2008/Nohl-DNS-privacy.pdf (o carregado em 18 de junho de 2013).

57 "A Arte de Enganar" é um livro de Mitnick voltado à utilização da engenharia social associada ao hackering (a edição brasileira, realizada pela editora Makron Books, é de 2003).

tão onipresentes hoje em dia), em lugares como cibercafés, lan houses, restaurantes, aeroportos, hotéis, trens, ônibus, entre outros. Ameaças semelhantes podemos enfrentar no nosso lugar de trabalho, já que ele é geralmente coletivo, embora o seja em uma escala efetivamente mais restrita que os lugares públicos.

Cabe ressaltar que é o método GET do protocolo http quem envia os parâmetros da requisição concatenados ao endereço URL. Isso pode revelar dados de identificação do usuário, caso o método GET esteja sendo utilizado para fazer login, por exemplo (esse tipo de identificação, entretanto, já é raro hoje em dia). Esses dados vão ficar no histórico de navegação. O método GET é muito utilizado em páginas de busca. Buscando-se, por exemplo, o termo "privacidade", a página do Google gera a seguinte requisição concatenada ao endereço URL:

http://www.google.com.br/search?hl=pt-BR&source=hp&biw=&bih=&q=privacidade&btnG=Pesquisa+Google

Deixando essa requisição no cache do navegador, revelamos nossos interesses em buscas abertamente a quem tenha acesso ao computador (além de fornecer essa informação ao provedor de serviço e ao próprio Google). A questão de gerenciar o cache do navegador é comumente negligenciada pelos usuários comuns. Os navegadores vêm com cache e cookies inicialmente habilitados. Os usuários geralmente não sabem que podem desabilitá-los ou removê-los ou como fazer isso e também não compreendem sua natureza e os riscos a ela relacionados.

O segundo grupo de ameaças, as do canal de comunicação, está ligado à possibilidade de varredura ou vigilância dessa comunicação, chamada de *sniffing* (significando literalmente "farejamento" em português). O *sniffing* é facilitado devido à construção de protocolos de rede, http em particular. O http não foi projetado para evitar ou combater ataques e possui apenas métodos básicos de autenticação e de verificação da integridade das mensagens (controle de erros). Os dados de formulários preenchidos em sites pelos usuários podem ser interceptados com a técnica do *sniffing* se não forem criptografados.

Observando o fluxo de informações de um computador durante um tempo prolongado, pode-se facilmente construir um perfil do usuário do computador em questão, ou, mais precisamente, do endereço IP atribuído ao computador. Aqui, não diferenciamos o que é transmitido: requisições de páginas HTML, cookies ou o próprio código HTML. A natureza do modelo do http é um problema do qual emergem vários outros problemas maiores.

Como já mencionado, o "farejamento" pode ser efetuado utilizando ferramentas gratuitas que são surpreendentemente potentes, embora sua aplicação não seja fácil para quem não conhece os modelos de protocolos utilizados na rede.

Levando em consideração a magnitude do fluxo de dados e sua posição na cadeia de comunicação pelo http, os provedores de acesso à rede têm a maior condição de interceptar a comunicação entre os seus clientes e os servidores de http por eles acessados. Em vários países, os provedores de acesso à rede são legalmente obrigados a manter por tempo prolongado os logs de todas as requisições efetuadas pelos contratantes do serviço. A União Europeia, por exemplo, lançou uma diretiva que define esse tempo, chamado de prazo de retenção de dados, passando de 6 meses a 2 anos[58]. No Brasil, até o momento, não há nenhum regulamento jurídico sobre essa questão, e os usuários permanecem completamente dependentes das políticas internas dos provedores. Assim, é claro que os provedores tendem a manter esses dados para construir e vender os perfis digitais de seus usuários, pois isso pode ser até mesmo mais lucrativo do que o seu serviço principal.

As ameaças à privacidade oriundas do servidor http estão ligadas ao conjunto de

58 Diretiva 2006/24/CE do Parlamento e Conselho Europeus, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicação eletrônica publicamente disponíveis ou de redes públicas de comunicação, e que altera a Diretiva 2002/58/CE.

informações que ele recebe do computador-cliente e que podem ser processadas e agregadas. Os servidores http geram arquivos de logs de visitas, em princípio por motivos puramente administrativos, mas eles podem trazer mais informações quando agregados com outras fontes de dados. Esses logs podem estar acessíveis também a outras pessoas além dos administradores dos servidores, podendo conter: IP do computador requerente, data e hora da chegada da requisição, URL solicitado, tempo de transmissão, nome associado ao usuário, erros na transmissão, dados sobre o tipo e capacidade do navegador, sistema operacional do computador requerente e o endereço de origem da navegação descrito a seguir (cabeçalho *Referer* do http).

3.2. 5. Scripts do navegador

Em dado momento, o HTML demonstrou-se revolucionário, mas logo a sua natureza estática tornou-se insuficiente para as crescentes aplicações da rede, particularmente as comerciais. Ele continua sendo a principal linguagem para a renderização de páginas WWW, mas já há tempos seu código pode ser manipulado com a utilização de outras linguagens que foram criadas para aumentar a "reatividade" das páginas. Simplesmente, o HTML, que é uma linguagem de definição do layout de páginas e não uma linguagem de programação, precisava de algum suplemento programático. Surgiram algumas linguagens de script para navegadores, dentre elas o JavaScript, desenvolvido pela Netscape em 1995, praticamente tornou-se a linguagem padrão. Com isso, o HTML evoluiu em uma variação sua denominada DHTML (HTML dinâmico). Além do JavaScript, temos ainda o ecmascript, o jscript e o vbscript, sendo os dois últimos a resposta da Microsoft ao seu antigo concorrente, a Netscape.

Cabe ressaltar que o JavaScript não tem muita relação com a linguagem Java além do fato de ambos terem herdado certas caraterísticas semânticas da linguagem C. O acréscimo de "-Script" pode sugerir que o JavaScript seja uma linguagem simplificada ou "atenuada". Nada mais errôneo. O JavaScript é uma linguagem moderna, voltada a objetos, pertencente ao conjunto das linguagens de programação de propósito geral e é muito potente. Além disso, ela é uma das mais populares e mais usadas em programação, de forma geral.

Quando usado em navegadores, o JavaScript não pode acessar recursos locais no computador do usuário, mas isso é mais uma caraterística e exigência da arquitetura programática dos navegadores do que do próprio JavaScript e das outras linguagens de script[59]. Mesmo assim, o JavaScript é suficientemente potente para escrever códigos capazes de colecionar vários dados sobre o usuário do navegador, observando seus padrões de navegação, por exemplo. Os scripts nos navegadores podem construir dinamicamente os elementos da página HTML, inclusive outros blocos de scripts. Isso dificulta a descoberta de códigos, objetos e elementos mal-intencionados que possam afetar a privacidade de usuários da rede. Os scripts podem, se permitidos pelo navegador, acessar, por exemplo, o conteúdo da área de transferência (conhecida como *"clipborad"*). Isso pode ser muito perigoso se considerarmos que os usuários, via de regra, não memorizam as suas senhas e as colocam nas caixas de texto nas páginas WWW de login com o uso do "copia-e-cola".

Os scripts são utilizados juntamente com outras tecnologias, como os cookies, para gerar web bugs e efetuar o web tracking, descritos a seguir, bem como numerosos outros tipos de ataques.

3.2.6. Cookies

Cookies, significando "bolachas" em português, são pequenas porções de informação textual que os servidores de http podem gravar no computador-cliente por meio do navegador

59 Alguns navegadores podem ser configurados para poder acessar os arquivos locais através de scripts e algumas bibliotecas adicionais, como a Microsoft Scripting, por exemplo. O padrão HTML5 prevê a possibilidade de acesso dos arquivos locais, mas ainda não é mantido por browsers além do Chrome.

que faz a requisição a esses servidores[60]. Inicialmente, eles foram utilizados para criar contadores de visitas, sondagens, lojas virtuais (cestas virtuais) e sites que requerem login e devem manter aberta a sessão. Logo, os cookies passaram a ser utilizados para monitorar as atividades dos usuários em suas visitas a sites e disponibilizar propagandas relacionadas.

O mecanismo de funcionamento dos cookies não é algo comumente conhecido e por isso gera confusão. Existe a convicção de que os cookies sejam uma fonte de vírus, o que não é possível, dado que os cookies são textos e não podem conter um código executável. Devido ao mesmo fato de não serem programas, os cookies não podem acessar recursos do computador, como arquivos no disco local.

O protocolo http, que serve para acessar arquivos na WWW, é um protocolo *sem estado*. Isso significa que uma simples requisição http de um cliente a um servidor não contém informações que permitam manter essa comunicação por tempo prolongado. O navegador do computador-cliente manda uma requisição contendo o endereço IP do servidor, o número da porta (80 identifica o protocolo http), o nome do recurso desejado (arquivo HTML, CSS, imagem, entre outros), seu próprio endereço IP e o número da porta a qual ele espera receber resposta. O servidor recebe essa informação, busca o recurso solicitado e o envia ao IP do cliente para a porta previamente indicada. Depois disso, o servidor (teoricamente) esquece tudo o que aconteceu, e o processo tem que se repetir para que o cliente obtenha mais arquivos. Isso gera problemas à natureza dos contatos dos usuários com os sites prestadores de algum serviço que devem reconhecer esses usuários. Os cookies surgiram para resolver esse problema, isto é, para introduzir no protocolo sem estado http a possibilidade de diferenciar as pessoas que visitam um dado serviço.

Conforme o modelo supramencionado de comunicação cliente-servidor, se o servidor tinha gravado o IP do cliente e esse IP mudou logo em seguida, o servidor na verdade não memorizou nada de valor do ponto de vista da identificação do usuário do serviço prestado. Isso, porém, não precisa ser verdade de outros pontos de vista específicos, como aqueles relacionados ao monitoramento do desempenho do servidor, à sua administração, à frequência de acesso a recursos e até mesmo à área geográfica da qual chegou a requisição. Como já mencionamos, os servidores de http normalmente guardam esse tipo de informação e seus administradores têm acesso a ela.

Os dados contidos nos cookies têm a forma de uma lista de pares nome/valor. Quando o servidor quer colocar um cookie no computador do cliente, ele envia um cabeçalho http com o comando Set-Cookie com os dados próprios do cookie. Um cookie gravado com êxito normalmente pode ser lido somente pelo servidor remetente dele, mas há outras modalidades de acesso. Os dados gravados em um cookie incluem:

- nome e valor atribuído a ele;
- domínio e caminho de acesso, que se referem à transmissão do cookie;
- prazo de validade (tempo de vida) do cookie, após o qual o navegador o removerá.

Para gravar um cookie, o servidor só necessita fornecer o nome dele. Se o domínio não for fornecido, o acesso ao cookie será concedido apenas ao servidor que o mandou gravar. Se o tempo de vida do cookie não for fornecido, o navegador deverá removê-lo na hora em que for fechado.

O mecanismo de cookies pode ser utilizado para ultrapassar a limitação do http para manter uma *sessão*. Por sessão entende-se o conjunto de comunicações http consecutivas e seus dados, entre o cliente e o servidor, no decorrer de algum tempo. O cliente e o servidor que trocam as informações contidas nos cookies reconhecem-se, sendo isso tanto importante para o servidor quanto para o cliente. Os cookies utilizados desse jeito chamam-se de cookies *de sessão*. Esse tipo de cookie é gravado quando o parâmetro Expires (expira) está vazio.

60 O conceito de cookie foi elaborado por Lou Montulli, um ex-empregado da Netscape, em 1994.

Os exemplos citados da utilização de cookies demonstram sua utilidade, mas infelizmente os cookies trazem consigo o risco de *spyware* (espionagem).

Existem cookies persistentes que se mantêm no computador por um tempo mais longo do que o tempo da sessão (o tempo de vida deles pode ser definido). Esses cookies vão ser enviados ao servidor cada vez que o usuário acessar o serviço prestado (se os cookies não tiverem sido removidos intencionalmente). Por isso, esse tipo de cookie pode servir para verificar quando o usuário navegou no serviço pela primeira vez e qual foi a frequência e o tempo de duração de visitas seguintes. Desse modo, pode-se rastrear os padrões de uso em um serviço. Frente a isso, esse tipo de cookie recebeu o nome de "cookie de rastreamento" (tracking cookie).

Os cookies podem ser criptografados quando a sessão é estabelecida através da versão segura do http, o https. Esses são chamados cookies seguros (secure cookies), não sendo tão suscetíveis a vazamento por meio de grampeamento da comunicação pelo http.

Os cookies podem ser divididos em diretos (first-party cookies) ou indiretos (third-party cookies). Os cookies diretos são gravados com o nome do domínio ou de seus subdomínios, o que fica indicado no endereço URL na caixa de endereços do navegador. Os cookies indiretos podem conter domínios diferentes daqueles contidos no endereço. Esses cookies geram muita discussão acerca da privacidade. Eles chegam de um site (ou são enviados a ele) diferente daquele atualmente visitado pelo usuário, o qual frequentemente sequer sabe disso. Esse outro site também pode ser chamado de indireto. As páginas HTML podem conter subpáginas embutidas em frames (quadros), através do elemento <IFRAME> ou <OBJECT>, e estas podem utilizar cookies. Conforme já mencionado, isso cria a possibilidade de rastreamento do uso da página com objetivos de marketing ou outros,. Os cookies indiretos podem ser de sessão ou persistentes. A Fig. 1 ilustra o uso desses cookies.

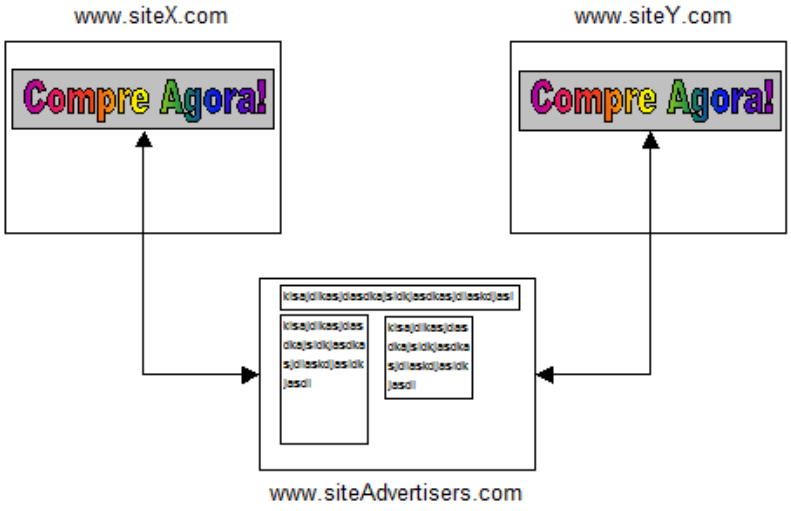

Fig. 1. Ilustração do uso dos cookies indiretos. O usuário visita duas páginas nos sites www.siteX.com e www.siteY.com. Os banners "Compre Agora!" são colocados no tag <IFRAME> e são carregados a partir do site www.siteAdvertisers.com. Quando o usuário visita qualquer um desses três serviços, os cookies são gravados e lidos pelo servidor www.siteAdvertisers.com. Assim, esse servidor pode construir o histórico das visualizações desse banner.

Cabe ressaltar que o servidor que grava o cookie não é obrigado a indicar o seu domínio no parâmetro Domain. Ele pode colocar o nome de um outro domínio. Os navegadores modernos podem, entretanto, controlar esse parâmetro e não permitir a gravação do cookie indireto. No FireFox, existe a opção de "Aceitar cookies de outros sites", que pode ser desmarcada, e, em princípio, as especificações de padrões RFC 2109[61] (antigo) e RFC 2965[62] (atualizado) requerem que os navegadores protejam a privacidade dos usuários e

61 D. Kristol, Bell Laboratories, Lucent Technologies, L. Montulli, Netscape Communications. Request for Comments 2109, HTTP State Management Mechanism. Network Working Group, fevereiro de 1997. http://www.ietf.org/rfc/rfc2109.txt (o carregado em 18 de junho de 2013).

62 D. Kristol, Bell Laboratories, Lucent Technologies, L. Montulli, Epinions.com, Inc. Request for Comments 2965, HTTP State Management Mechanism. Network Working Group, outubro de 2000.

deixem essa opção desmarcada nas configurações-padrão. Mas isso não é uma realidade e vários navegadores têm essa opção automaticamente habilitada.

De fato, as empresas de propaganda na internet utilizam os cookies indiretos extensivamente para rastrear os usuários que visitam as páginas onde essas empresas colocaram seus anúncios. Os cookies indiretos não são a única maneira de rastrear os usuários. Existe também o assim chamado web bug, descrito a seguir (na realidade, essas técnicas se complementam na execução do *web tracking*). Sabendo quais sites com as propagandas específicas os usuários visitam, as empresas podem fazer inferências a respeito de suas preferências, criar seus perfis virtuais e individualizar as propagandas a eles direcionadas, até mesmo diferenciando preços para esses usuários (isso soa particularmente injusto). Além disso, os usuários acabam deixando muito mais informações sobre si mesmos, o que facilita a criação dos seus perfis.

As empresas que utilizam cookies indiretos às escondidas correm risco de perder a confiança dos clientes, como demostra Miyazaki[63].

Existe mais uma variação de cookie que já pode ser classificada como um *malware* regular. Utilizando scripts e outras tecnologias que podem ser aplicadas em páginas HTML (como o Flash, por exemplo), podem ser criados cookies que conseguem sobreviver às tentativas de serem removidos (remoção, esta, que todos os navegadores deveriam conseguir realizar). Esse tipo de cookie foi batizado de cookie zumbi (zombie). Esse cookie, ao ser criado, grava seu conteúdo em outros possíveis lugares e, depois de ser removido de um ou de alguns lugares, restaura-se, utilizando suas várias cópias, e tenta ainda restaurar todas as cópias que foram deletadas. Isso é possível, pois o termo cookie já não pode ser atribuído somente aos cookies http do servidor. O Flash dispõe de um espaço no disco local que serve para criar buffers dos streams de multimídia carregados da internet. A linguagem HTML na versão 5 também prevê a existência de um espaço hierárquico para armazenamento local no computador do usuário. Existe um exemplo de cookie zombie particularmente difícil de ser removido. Ele foi batizado de evercookie (cookie eterno) e tem forma de um aplicativo escrito em JavaScript. O autor desse código, que é público, é também autor do *Samy Worm*. O evercookie foi publicado em setembro de 2010. Ele utiliza treze tecnologias para se replicar[64].

Uma combinação da negligência dos riscos por parte dos usuários, dos defaults dos navegadores e da sofisticação e onipresença dos cookies faz destes uma técnica que tem gerado muitas preocupações acerca de privacidade e que, por essa razão, já resultou em várias ações legislativas[65].

É interessante constatar como essa tecnologia potencialmente tão perigosa recebeu um nome tão "meigo". Algo psicologicamente semelhante (e não obrigatoriamente intencional, embora seja difícil afirmar isso com certeza absoluta) ao que aconteceu no caso da computação em "nuvem".

3.2.7. Cabeçalho Referer do protocolo http

Entre as ameaças à privacidade de usuários da rede deve-se ainda incluir o cabeçalho *Referer* do protocolo http. O nome desse cabeçalho contém um erro ortográfico (deveria ser "referrer" – "referente", ou melhor, "requerente anterior") que foi cometido na documentação RFC 1945 e, desde então, espalhou-se nas implementações do http. Infelizmente, para manter

http://www.ietf.org/rfc/rfc2965.txt (o carregado em 18 de junho de 2013).

63 Anthony D. Miyazaki. Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage. 2008, American Marketing Association, Vol. 27 (1) Spring 2008, 19–33.

64 A Wikipédia inglesa. http://en.wikipedia.org/wiki/Evercookie (o carregado em 18 de junho de 2013).

65 Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:pt:HTML (carregado em 23 de junho de 2013).

a corretude tecnológica no presente texto, teremos que reproduzir essa forma errônea.

Enquanto alguns usuários comuns sabem da existência de cookies e de scripts, mesmo que suas funções não estejam claras para eles, a consciência relativa à existência, à função e aos perigos relacionados ao cabeçalho *Referer* é quase nula. Quando visitamos uma página, os navegadores recordam o endereço URL dela. Quando navegamos dessa página a uma outra, clicando, por exemplo, em um link, o navegador preenche o cabeçalho da requisição http Referer com aquele endereço URL gravado e o envia ao servidor da página em cujo link clicamos. Desse modo, o servidor receberá a informação de onde vem o usuário. Gravando essa informação no computador-servidor juntamente com o endereço IP ou outras informações que possam acompanhar a requisição (cookies), pode-se reconstruir a rota de navegação do usuário. O preenchimento desse cabeçalho pelos navegadores, conforme o padrão de http, não é obrigatório, e o usuário deve ter a opção de escolher como tratar esse cabeçalho. Os navegadores mais utilizados já não habilitam o envio deste cabeçalho, pois isso gerava preocupações justificadas em relação à privacidade. O navegador FireFox, por exemplo, permite redefinir sua ação relativa a esse cabeçalho no parâmetro "network.http.sendRefererHeader", acessado com o endereço especial "about:config". O Internet Explorer não envia esse cabeçalho a menos que seja no modo https[66].

Todas as ações supramencionadas e suas eventuais consequências são fortemente ligadas aos softwares que servem para interação com a rede aberta – os navegadores.

3.2.8. Navegadores

Os navegadores são elementos arquitetônicos centrais na discussão sobre privacidade na rede aberta. Como quaisquer softwares, eles não podem garantir segurança absoluta. Além disso, eles, mesmo sendo gratuitos, ou mesmo pertencendo à categoria de software livre, são comerciais, pois geram lucros para os seus autores. A natureza comercial desses softwares, bem como de muitos outros modelos de negócio que se desenvolveram graças à rede aberta, não é algo geralmente conhecido pelos usuários leigos. Como já sinalizamos, informação equivale a poder, e os navegadores são ferramentas pelas quais essa informação passa de um indivíduo a outros indivíduos ou serviços. Quem é dono de uma dessas ferramentas, tem um poder enorme nas mãos. Com certeza, essa observação não se limita aos navegadores. Qualquer software popular ou até mesmo qualquer tecnologia amplamente utilizada, quando controlados centralmente por um ou alguns donos, trazem a eles excesso de poder.

A questão da avaliação da quota de mercado de navegadores não é simples. As estatísticas publicadas na rede variam muito, mas, em setembro de 2012, o mercado de navegadores mostrou-se um mercado de apenas três jogadores: Google (Chrome), Microsoft (Internet Explorer), e Mozilla Foundation (FireFox), pois eles juntos ultrapassaram 75% da quota de mercado[67]. É sensato aceitar que uma quota total maior do que 50% seja suficiente para identificar os principais jogadores, desse modo a quota atual de 75% já sinaliza que o mercado de navegadores é um oligopólio que, a propósito, apresenta certos fortes sintomas de cartelização.

A presente monografia não avalia qual dos navegadores é o melhor, por causa, antes de tudo, da existência de muitas dimensões para estimar suas qualidades, influência no mercado, ligação às normas de implementação e padrões de codificação. A situação muda constantemente, os donos dessas tecnologias entram em alianças e depois as rompem. Parece justo afirmar que enfrentamos uma "guerra comercial" entre navegadores (seus donos). A lógica do mercado, ao que parece, deve nos fornecer algumas dicas. Certamente, do ponto de vista do mercado livre, devemos acreditar que os próprios usuários, fazendo suas escolhas,

66 http://support.microsoft.com/kb/178066 (acessado em 6 de fevereiro de 2013).

67 Existem várias fontes para essas estimativas, uma deles é a Wikimedia, que tem um grande número de usuários. O artigo (atualizado com regularidade) fica no seguinte endereço: http://en.wikipedia.org/wiki/Usage_share_of_web_browsers.

efetuam estatisticamente a melhor avaliação desses softwares, e muitos usuários concordam com essa dimensão de medida. No nosso discurso, é importante indicar as caraterísticas dos navegadores que podem afetar a privacidade dos usuários.

Essas caraterísticas são numerosas e estão relacionadas tanto à proteção da privacidade quanto à possibilidade de sua invasão. Todos os navegadores oferecem possibilidades de controlar as questões relacionadas à privacidade[68], mas o problema está no fato de que os usuários em geral parecem não utilizá-las, sendo as configurações-padrão (*defaults*) aplicadas no momento da instalação frequentemente fixadas de forma desfavorável nesse sentido.

A questão dos assim chamados *defaults* em *softwares* (supostamente) livres é mais complicada do que parece à primeira vista. O FireFox é comumente percebido como um *browser* livre, mas só devido ao fato de permitir o motor de busca do Google como *default* durante a instalação esta paga aos donos do FireFox (à Mozila) por esse serviço. O FireFox é sim gratuito no que diz respeito ao seu carregamento no computador e utilização, mas será que não estamos pagando com a nossa privacidade?

Negócios como esse firmado entre o Google e a Mozilla são sintomáticos. Existe uma verdadeira batalha de navegadores, motores de busca e outras tecnologias e empresas que desejam nos controlar e, com isso, ganhar dinheiro em uma quantia verdadeiramente exorbitante. Nessa guerra por dinheiro, ainda veremos muitas confrontações e alianças temporárias. Cabe ressaltar que o navegador Chrome do Google é evidentemente o competidor do FireFox. Mesmo assim, o Google vê vantagens em pagar à Mozilla além do que é investido na divulgação do seu próprio navegador.

Na época digital vários softwares, páginas de internet, downloads e outros serviços e recursos parecem e são frequentemente apresentados como gratuitos. Nós aceitamos essas ofertas, esquecendo-nos do tão simples fato de que neste mundo não há nada de graça. O que realmente acontece na rede aberta, entre os usuários e os donos de serviços, foi parafraseado na seguinte afirmação, que ficou bastante popular em 2010 graças a um usuário da rede[69]: *"If you are not paying for it, you're not the customer; you're the product being sold."*

Efetivamente, o problema dos navegadores no que diz respeito à privacidade está ligado ao seu modelo de negócio e ao fato de esse negócio estar dominado no mercado por alguns poucos jogadores cuja atividade principal já causa preocupações sérias na questão da privacidade. Na rede aberta, como já mencionamos, as ameaças à privacidade estão ligadas à revelação de dados pessoais ou de outros tipos de dados, que, quando processados e agregados, podem tornar-se pessoais. Se esses dados tem em um formato imediatamente legível aos humanos, como o de um texto plano, são transmitidos por protocolos como o http, isto é, de um computador a um outro, cujos endereços IP são conhecidos e reconhecíveis geograficamente, quando esses dados são interpretados pelos navegadores contemporâneos subordinados ao mundo comercial, a situação parece, por definição, crítica.

3.3. Coleta de dados cadastrais

A coleta de dados cadastrais acontece em várias situações na vida cotidiana, não só por meio da rede. Nas economias desenvolvidas, os cidadãos precisam se cadastrar e depois se identificar utilizando os dados cadastrais praticamente a todo momento. Eles precisam disso para telefonar, ver TV a cabo, viajar de avião, ônibus, trem ou outro meio de transporte público, utilizar os serviços do banco, de uma empresa, instituição pública, biblioteca, hotel,

68 Pelo menos, em computadores comuns. A questão de branded devices não é tão clara – nem sempre podemos instalar neles os add-ons que servem para aumentar a privacidade.

69 No link a seguir, acessado em 28 de janeiro de 2013, http://www.metafilter.com/95152/Userdriven-discontent#3256046, o autor dessa frase aparece com o nome de "blue_beetle", mas ele foi depois revelado como sendo um tal de Andrew Lewis, que, a propósito, tornou-se logo em seguida um comerciante de camisetas estampadas com essa frase popular.

ou ainda para comparecer a uma consulta médica, comprar algo com cartão, entre outras situações.

A coleta de dados pessoais a fim de manter o cadastro dos usuários é onipresente também na rede aberta. A maioria dos sites oferece ou exige que o usuário crie conta com login e senha, mas frequentemente também com dados pessoais, como demográficos (nome, idade, profissão) ou de comunicação (número de telefone, e-mail). Os usuários tendem a abrir mão de sua privacidade e comumente fornecem mais dados sobre si do que é objetivamente necessário, inclusive fornecendo *dados verdadeiros*.

A identificação de clientes ou usuários de serviços por meio de cadastro é tão onipresente que já não causa surpresa. Mas é esse cadastro que abre caminho na rede aberta para o perfilamento de usuários.

Uma outra observação é a de que nós deixamos nossos dados sensíveis ao nos cadastrar ou nos identificar em um número enorme de lugares. É difícil estimar esse número, mas com certeza podemos suspeitar de que os nossos dados como usuários da rede existam separadamente, em várias configurações, em centenas de bancos de dados cuja localização física é praticamente desconhecida. Esses dados não são diretamente visíveis para nós, então não sabemos se estão corretos ou atuais e nem o que os donos dos bancos de dados e outras pessoas ou entidades fazem ou podem fazer com eles. O nosso controle sobre essas nossas "imagens digitais" é efetivamente muito baixo, se não nulo. As possibilidades de identificar os usuários e de individualizar as propagandas são razões para o florescimento do marketing individualizado.

Mais uma questão relacionada ao cadastro que pode ter implicações na nossa privacidade é o fato de que, via de regra, precisamos cadastrar-nos em muitos lugares, não apenas na rede. Isso gera o problema da memorização de logins e senhas. O usuário comum tem que lembrar logins, senhas, códigos ou chaves para acessar o seu computador, telefone celular e outros dispositivos portáteis, pagar ou sacar dinheiro com cartão, acessar a conta bancária, ter conta de e-mail, entrar em uma rede social, acessar o site da clínica ou laboratório de análises, da escola dos filhos e até mesmo para abrir a porta do bloco onde mora ou da sala na qual trabalha. Frequentemente, temos mais do que uma conta bancária, mais do que um cartão de crédito ou débito, mais do que um endereço de e-mail ou participamos de mais do que uma rede social, entre outros exemplos. O número dessas chaves pode facilmente ultrapassar mais de dez. Por isso, já surgiram softwares[70] para centralizar o gerenciamento de dados de acesso com o uso de uma única senha. Isso facilitaria a nossa vida, mas é muito mais arriscado do que ter esses dados gravados separadamente em vários lugares e criptografados ou guardados no papel em lugares seguros. Os softwares desse tipo, em teoria, deveriam, também, lidar com um problema que ocorre quando, para acessar um site ou recurso, digitamos por acaso os dados cadastrais existentes e corretos, mas de um outro site ou recurso do nosso interesse. O excesso de senhas e outros códigos é um problema dos usuários mais conscientes dos riscos. Infelizmente, os usuários comuns tendem a utilizar a mesma combinação de nome/senha para acessar seu computador, todos os acervos na rede, bem como outros recursos fora dela.

Assim, a "digitalização" da nossa vida implica, consequentemente, na excessiva "loginização" e "senhação" dela, o que é difícil de gerenciar e pode gerar riscos à segurança dos nossos dados e comprometer nossa privacidade. A questão não se refere apenas ao gerenciamento, por nós mesmos, dos nossos dados cadastrais e de outros relacionados, mas também à possibilidade de vazamento desses dados dos acervos na rede, o que acontece com

70 A wikipédia portuguesa contem o artigo "Gerenciadores de senhas" que descreve a essência desta categoria de software - http://pt.wikipedia.org/wiki/Gerenciadores_de_senhas (carregado em 18 de junho de 2013), mas, infelizmente, omite o tema importante de suas vulnerabilidades, o qual podemos encontrar na versão inglesa "Password manager" - http://en.wikipedia.org/wiki/Password_manager (carregado em 18 de junho de 2013).

frequência e em uma escala alarmante. Em 2012, houve dois vazamentos significativos desse tipo: do Yahoo, vazaram 450.000 senhas em julho[71] e, da LinkedIn (juntamente com a eHarmony), em junho com as estimativas de 6,5 milhões de senhas reveladas (o número de vítimas é difícil de estimar, pois as senhas se repetem, mas a rede social em questão tinha 160 milhões de usuários – possíveis vítimas)[72]. Cabe ressaltar que no caso do vazamento da LinkedIn, foi publicada uma lista de dez senhas mais populares utilizadas pelos usuários, nomeadamente (na ordem de menos a mais utilizadas): sex, ilove, the, angel, 12345, job, god, work, 1234, link[73].

Devemos frisar que a confiabilidade das informações sobre vazamentos de dados é sempre discutível e temos que lidar com suposições e até fofocas. As empresas afetadas não querem revelar detalhes para não queimarem a sua imagem no mercado ainda mais.

3.4. Web tracking (web bug) e perfilamento de usuários

O web bug, literalmente "inseto de rede", às vezes denominado "grampo de rede"[74] em português, é um objeto colocado em uma página web que permite verificar se um usuário abriu essa página. Essa técnica permite realizar ações com o mesmo objetivo dos cookies de terceiros. Originalmente, web bugs surgiram na forma de arquivos de imagens, como gif ou jpg, mas hoje em dia existem outras modalidades, como scripts locais executados por navegadores, tags OBJECT, entre outras. Web bugs aparecem na literatura com vários outros nomes: *tracking bug*, *web beacon, tag* or *page tag*. As variações de web bug que utilizam arquivos de imagem são chamadas de: *tracking pixel* (pixel de rastreamento), *pixel tag*, *1×1 gif* e *clear gif*[75].

O web bug pode ser utilizado em páginas HTML, mas isso não significa que os riscos aparecem somente quando navegamos por vontade própria pela internet. Os programas modernos de e-mail são capazes de exibir conteúdos de mensagens em formato textual ou mesmo em HTML (além de poder conter, como anexos, arquivos em qualquer formato). Exibindo mensagens em HTML, os programas de e-mail atuam como navegadores. Na realidade, eles utilizam o código de um navegador e mais correto seria afirmar que eles são de fato navegadores, nesse caso. Desse modo, qualquer tipo de ameaças referente a http e HTML já descritas, referem-se também aos e-mails em formato HTML. Infelizmente, a rápida "internetização" de várias ferramentas de software, como o pacote Microsoft Office, Open Office e numerosas outras, amplia essas ameaças em gravidade, pois esses programas permitem escrever em código HTML e navegar. Um dos programas que têm capacidade plena de um navegador é o tão popular *Skype*.

O web bug embutido na página fica normalmente invisível ou de difícil percepção ao usuário. Ele pode estar escondido, como script, ou ter tamanho mínimo, como o de uma imagem gif de 1×1 pixel de tamanho. Ele permite, a quem o colocou na página, verificar se

71 Brad Reed, BGR News para Yahoo News! 450,000 Yahoo passwords just got hacked; find out if you might be affected, de 12 de julho de 2012. http://news.yahoo.com/450-000-yahoo-passwords-just-got-hacked-might-155505616.html (carregado em 18 de junho de 2013).

72 Sem autoria indicada, BBC NEWS Technology de 6 de junho de 2012 - http://www.bbc.co.uk/news/technology-18338956 (carregado em 18 de junho de 2013).

73 Anthony Wing Kosner, Unbelievable: Top Ten Hacked LinkedIn Passwords, Forbes, de 6 de novembro de 2012 - http://www.forbes.com/sites/anthonykosner/2012/06/11/unbelievable-top-10-hacked-linkedin-passwords/ (carregado em 18 de junho de 2013).

74 O grampo pode compreender a escuta de comunicação pelos protocolos de rede – algo ainda mais severo. Essa tradução do inglês "bug" se dá a partir de um segundo possível sentido seu, que é figurativo.

75 Richard M. Smith, The Web Bug FAQ - http://w2.eff.org/Privacy/Marketing/web_bug.html (link acesado em 18 de junho de 2013).

um usuário abriu essa página ou um e-mail em formato HTML[76]. Assim, podem-se rastrear visitas a páginas e aberturas de e-mails.

Utilizando web bugs, empresas de rastreamento de usuários da internet podem obter várias informações, como:

- endereço IP;
- nome do *host* (o domínio de onde foi carregada a página), utilizando o cabeçalho Referer (descrito no ponto 3.2.1.7.);
- dados sobre o sistema operacional em que está sendo executado o navegador;
- dados sobre o tipo e a versão do navegador;
- data e hora em que a imagem ou o script foram carregados;
- informação sobre outros sites visitados, caso cookies estejam habilitados e acessíveis ao domínio da empresa de rastreamento.

A idéia por traz do web bug é muito simples. Colocando em uma página o seguinte código HTML:

```
<img src="http://www.rastreadorX.com/webbug.php?alguns_dados"/>
```

o dono do domínio www.rastreadorX.com faz o navegador do usuário carregar o arquivo de uma imagem, mas, com isso, o navegador efetua uma requisição à página de script de servidor webbug.php. Este script vai receber como parâmetro alguns_dados. Esses dados podem ser os supramencionados e podem ser gravados pelo servidor em um banco de dados, acumulando cada vez mais informações para a elaboração do perfil digital do usuário.

Essas técnicas são utilizadas em massa, e o web tracking é um dos negócios online que mais cresce atualmente. Cabe ressaltar que a página inicial da Universidade de Brasília contém código script, escrito em JavaScript, que efetua web tracking para o domínio googleanalytics.com (Fig. 2). Isso é muito modesto quando comparado à página mostrada na Fig. 3.

Fig. 2. Página inicial do site da UnB carregada em 26 de setembro de 2012, mostrando o web bug.

Fig. 3. Página do serviço www.businessinsider.com carregada em 1° de outubro de 2012, mostrando trinta web bugs detectados pelo suplemento Ghostery (com bloqueio desabilitado – haja vista os nomes não riscados).

76 Devemos apontar que vários programas de email permitem bloquear as imagens em emails em formato HTML e oferecem filtros de spam, phishing, etc., mas para a proteção efetiva os usuários têm que entender os riscos e adotar os padrões adequados de comportamento e saber utilizar estas opções. Isso é muito raro.

O perfilamento de usuários é efetivamente igual à sua observação constante em suas atividades diárias e gravação dessas observações. Podemos imaginar uma situação em que isso possa ser necessário: órgãos do Estado observam, por exemplo, mediante autorização, um suspeito de ter cometido um crime gravíssimo durante sua interação com a rede. Mas fazer isso em massa para com todos os usuários da rede já soa altamente imoral. Fazer isso por motivos comerciais é ainda mais imoral (sobre esse aspecto, trata mais a fundo o item 3.3.1.1. Marketing individualizado).

3.5. Web spiders e spam

A palavra spam é mais um anglicismo que se radicou em vários idiomas do mundo, na atualidade. O termo significa a utilização de sistemas eletrônicos de comunicação para enviar mensagens indesejáveis, particularmente de propaganda. Cabe ressaltar, extrapolando para além da definição, que toda e qualquer mensagem de propaganda com altíssima probabilidade será indesejável. O spam nasceu dentro dos grupos de discussão Usenet, mas hoje já se espalhou e diz respeito antes de tudo ao sistema de e-mail.

Os *spammers* coletam os endereços de e-mail dos usuários, que são deixados na rede aberta quando nos cadastramos em sites ou participamos de discussões, entre outras formas. A coleta desses endereços tornou-se automatizada com o advento de programas que vasculham páginas da internet em sua busca – os *web spiders* (aranhas da rede). Existem ainda outras denominações a esses softwares (que, a propósito, podem efetuar qualquer outro tipo de

pesquisa metódica e dedicada, não apenas a busca por endereços de e-mail), tais como *web crawlers*, *harvesters, ants*, *scutters, robots, bots* ou indexadores automáticos. Esses programas são utilizados também por empresas para coletar informações sobre a sua concorrência.

A invasão da nossa privacidade com spam tem pelo menos três aspectos: primeiro, o spam é resultado do uso do nosso endereço de e-mail com outro propósito do que foi inicialmente presumido; segundo, o spam sobrecarrega os nossos recursos computacionais e de comunicação; e, terceiro, ele, ao ser removido ou tratado de qualquer outro modo, toma o nosso tempo. O aspecto da invasão à propriedade também pode ser considerado, pois quando temos que acessar o nosso e-mail com uso da rede celular comum, os provedores do serviço frequentemente cobram taxas elevadas pela transmissão de dados, por exemplo quando utilizamos roaming fora do nosso país ou utilizamos os cartões SIM pré-pago. Nestes casos, carregando e-mails de spam simplesmente perdemos dinheiro.

3.6. Software malicioso

O software malicioso (malware) é a categoria de invasão a computadores mais reconhecida pelos usuários comuns, embora estes frequentemente utilizem o termo "vírus" para descrever qualquer tipo de malware e, também, para dados que lhes possam parecer perigosos, como cookies ou objetos, como web bugs, que não são códigos executáveis. Os usuários comuns também costumam misturar o termo vírus com técnicas de ataque como o phishing, por exemplo. Do outro lado, os softwares antivírus tendem comumente a combater todos os tipos de malware, não apenas os vírus, como o seu nome poderia sugerir.

Não é possível fazer uma descrição completa dos malwares existentes atualmente. A questão relativa à sua classificação e aos seus riscos é altamente discutível. Existem pesquisas que visam à automatização desse processo com o uso de computadores[77], mas, de fato, ainda não existem definições uniforme satisfatórias do que são vírus e *worms*, por exemplo. Mesmo o número de malwares é muito difícil de se estimar, não mencionando o número de suas cópias espalhadas por máquinas em todo o mundo ou por computadores invadidos que servem para esconder e intermediar os ataques, os assim chamados "computadores-zumbis". A mesma limitação existe na avaliação dos danos financeiros causados por malwares, pois, para muitas empresas comerciais, o fato de ter sido vítima de um ataque pode provocar danos à sua imagem no mercado e trazer consequentemente ainda mais danos financeiros.

O quadro tecnológico de softwares modifica-se constantemente, bem como as possibilidades de invasão. Novos softwares legítimos, como versões e atualizações de sistemas operacionais, navegadores, pacotes de escritório e muitos outros, surgem com bastante frequência. Eles consertam as brechas descobertas, mas acabam introduzindo novas. Os malwares são desenvolvidos para atacar softwares legítimos que apresentam vulnerabilidades, sendo estas logo em seguida eliminadas, o que promove o surgimento de novas versões dos softwares legítimos e, consequentemente, de malwares contra eles e esse "jogo de gato e rato" repete-se infinitamente. O que permanece imutável é a nossa suscetibilidade humana a manipulações psicológicas, incluindo à engenharia social, nossa natureza sempre ligeiramente preguiçosa, nossa ingenuidade, crença na benevolência dos outros, eterna falta de tempo e a realidade cada vez mais virtual cheia de perigos difíceis de prever, entender e combater, e, finalmente, nossa posição no mundo conectado pela misteriosa rede ultraveloz de computação que engana nossos instintos humanos.

Devemos voltar aqui à observação relativa às ameaças da tecnologia. Tão frequentemente discutimos sobre vírus, programas de antivírus, segurança, riscos, privacidade, entre outros assuntos, e tão raramente enxergamos que, por trás disso tudo, existe

77 Por exemplo, Automated Classification and Analysis of Internet Malware; [Bailey, Oberheide, Andersen, Mao, Jahanian, Nazario] do Departamento da Engenharia Elétrica e Ciência da Computação da Universidade de Michigan, EUA.

e progride neste mundo um exército de pessoas profundamente deterioradas moralmente, que dedicam o seu tempo à criação de todos esses códigos maliciosos, trabalho, este que exige conhecimento técnico verdadeiramente extenso e que poderia estar sendo utilizado com o objetivo de tornar este mundo um lugar um pouco melhor. Essas pessoas, via de regra, permanecem impunes, a menos que tenham a ousadia de desafiar e atacar entidades governamentais de países desenvolvidos, suas agências de segurança pública, em particular.

Voltando à questão de como estimar o número de riscos oriundos dos malwares, podemos apenas citar alguns dados estatísticos cuja confiabilidade é sempre discutível. A empresa Symantec Corporation, por exemplo, que é a maior no segmento do mercado de softwares antivírus atualmente, publica dados sobre os malwares existentes e que estão sendo descobertos diariamente, bem como sobre os casos de ataques comunicados a computadores equipados com o software dessa empresa[78]. Muitos desses malwares são mutações de códigos já existentes ou de códigos antigos, já que os softwares que eram alvos de ataques já não são mais utilizados. Vale a pena enfatizar que os códigos maliciosos podem automodificar-se (realizar mutação), o que, via de regra, não altera sua essência lógica e objetivo de ataque, mas sim modifica sua caraterística numérica, comumente denominada "assinatura digital" (aqui no sentido de resumo simbólico, e não autenticador por criptografia assimétrica). Em setembro de 2012, o programa antivírus da Symantec Corporation (Symantec Endpoint Protection) informava a respeito de mais de 76 mil riscos conhecidos e combatidos por ele (os dados atuais podem ser encontrados no site da empresa).

A maioria dos malwares tem como alvo a plataforma do Windows, mas todos os sistemas são afetados, inclusive os mais novos, projetados para as plataformas portáteis, como o Android. Dados da Kaspersky Labs, referentes ao período que vai do segundo trimestre de 2011 ao segundo trimestre de 2012, indicam que o número de malwares reportados cresceu mais de 16 vezes[79]. Estamos presenciando o advento de uma nova onda de malwares, desta vez "móveis".

Os estudantes das disciplinas introdutórias de Informática, ao se familiarizarem com a questão dos malwares e da segurança dos sistemas computadorizados, fazem muitas perguntas do tipo: "O que os vírus podem fazer?". A melhor resposta é: tudo o que o programador mal-intencionado puder imaginar, e essa imaginação pode impressionar. Exemplos reais podem ser extremamente esquisitos. O vírus denominado Virus.MSWord.Beast (conforme a Netgear) infecta arquivos do Word, intercepta os eventos do relógio do sistema Windows e, entre 21:36 e 07:12 da manhã, abre e fecha a gaveta de CD-ROM durante duas horas sem parar[80]. O famoso worm Stuxnet espalha-se pelos memory sticks e infecta apenas os drivers PLS da Siemens que eram utilizados, por exemplo, nos computadores que controlavam as centrífugas de purificação de urânio no Irã (quase 60% das infecções confirmadas ocorreram no Irã)[81]. O ataque teve a intenção de aumentar a velocidade dessas centrífugas, o que comprometeria o processo da purificação. Não seria possível elaborar o tal malware sem a colaboração dos programadores desse driver e das entidades governamentais interessadas na execução desse ataque, cujos motivos políticos são óbvios. Surge aqui uma observação intrigante. Se até mesmo agências governamentais podem efetuar ataques desse tipo, como devemos nos proteger contra as invasões à nossa privacidade? A quem devemos recorrer para defender os nossos direitos mais fundamentais? Ao Estado, que aparentemente pode planejar e financiar tais atividades? Isso seria semelhante a pedir que um hacker nos protegesse contra ele mesmo.

78 http://www.symantec.com/threatreport/ (acessado em 5 de janeiro de 2013).

79 Os dados estatísticos podem ser encontrados no endereço (carregado em 28 de janeiro de 2013): http://www.kaspersky.com/about/news/press/2012/Android_Under_Attack__Malware_Levels_for_Googles_OS_Rise_Threefold_in_Q2_2012.

80 Netgear Procecure. Threat Monitor Virus.MSWord.Beast. http://prosecure.netgear.com/resources/threat-monitor-detail/Virus.MSWord.Beast?page=188 (carregado em 18 de jungo de 2013).

81 Wikipédia inglesa, artigo Suxnet, http://en.wikipedia.org/wiki/Stuxnet (carregado em 18 de junho de 2013).

Devemos enfatizar que essa observação não tem nada a ver com a avaliação dos eventuais riscos oriundos do programa nuclear iraniano do ponto de vista da segurança internacional. Falamos aqui sobre as possibilidades de ataques gerenciados e financiados pelos Estados, que, ao mesmo tempo, elaboram leis para a proteção de privacidade. Frente ao alvo do ataque supramencionado e aos acervos de conhecimento envolvidos, aos agentes decisivos e, por último mas não menos importante, ao dinheiro gasto, será que as nossas expectativas de proteção da privacidade na rede não são de certo modo exageradas?

O fato de se invadir o computador de um usuário com um malware qualquer já configura violação aguda de sua privacidade, pois, desse modo, invade-se sua propriedade. Podemos comparar a instalação de um malware no computador de um usuário com a invasão de sua casa e posicionamento nela de vários objetos com finalidades obscuras, incluindo câmeras, grampos, ou a manipulação, roubo ou destruição de objetos do proprietário. Os usuários experientes e, particularmente, os especialistas em TI ficam extremamente preocupados ao descobrirem qualquer software não desejado em seus computadores, seja ele malicioso ou simplesmente alheio. Os usuários leigos, ao contrário, segundo também a própria prática na área de TI do autor, continuam utilizando normalmente seus computadores, que já à primeira vista estão totalmente dominados por dezenas de programas maliciosos. Surge aqui uma observação de caráter ético. Na época digital, a segurança não é "pessoal", de um usuário e de seu computador. O computador desprotegido pode contaminar outros computadores ou servir como elo intermediário para tais ataques. Nesse contexto, somos todos responsáveis pela segurança da rede, embora essa responsabilidade não seja algo comumente percebido e compartilhado.

3.7. Software de espionagem (spyware)

Esta categoria de software pode ser maliciosa ou não. A diferença não depende só do fato de ele ser instalado de maneira sigilosa ou explícita.

O spyware malicioso seria aquele que é instalado sem o consentimento do usuário, ou não estando este consciente de sua função, e que monitora suas ações e informa aos autores ou donos desse software sobre essas ações, sendo essa informação então utilizada contra o interesse do usuário, de certo modo. As informações enviadas podem se referir a endereços de sites visitados, dados pessoais como números de cartões de crédito e débito, logins e senhas, endereços de e-mail ou até mesmo qualquer outro arquivo ou dado. Às vezes, esses softwares podem inclusive mandar spam ou exibir propagandas. Os mais conhecidos são: Aureate, Cydoor, Gator, Promulgate e SaveNow. A maioria deles é desenvolvida para a plataforma Windows, mas, como já mencionamos, a situação está mudando com a rápida expansão dos dispositivos portáteis com o sistema Android.

O spyware pode ser instalado no computador de um usuário e esse usuário pode estar ciente disso e até ser obrigado a subordinar-se a tal configuração. Isso acontece em muitos lugares de trabalho. Um exemplo de software desse tipo é o Spector[82], que grava todas as ações do usuário do computador e as envia ao servidor-controlador. O Spector foi inicialmente projetado para proteger crianças vigiando-as durante a sua interação com a rede (descobrir se elas sofrem abusos, usam drogas, têm problemas psíquicos, entre outros), então podemos crer que existem situações em que spywares podem ter o seu lado positivo.

Na internet surgem informações sobre práticas do mesmo tipo exercidas pelas empresas produtoras de smartphones e tablets, mas, na realidade, todos os programas que, de alguma forma, conectem o cliente com o produtor de um bem ou prestador de serviço são passíveis de desconfiança quanto a serem ou não spywares. Os softwares "gratuitos" frequentemente têm a opção de "participar do programa de aperfeiçoamento do software".

82 A página do produtor contem a descrição detalhada deste software. http://www.spectorsoft.com (acessado em 5 de fevereiro de 2013).

Nesse caso, os programas em questão podem enviar comunicados sobre erros às empresas desenvolvedoras. Além disso, todos os programas que gerenciam atualizações automáticas podem reenviar aos donos dados sobre o estado do seu equipamento, entre outras ações.

Tablets, smartphones, leitores de ebooks estão frequentemente ligados ao software de uma única empresa (branded devices), como a Microsoft ou o Google e particularmente a Apple. Esses dispositivos já vêm pré-configurados de tal maneira que várias ações do usuário possam ser observadas.

3.8. Localização física de pessoas

Conforme já mencionado, a distribuição geográfica de endereços IP é conhecida. Ela é suficiente para se localizar o portador de um endereço IP, e essa realidade é utilizada pelos servidores de http para a exibição de páginas no idioma da região de onde vem a requisição. Mas a internet já migrou para vários outros tipos de dispositivos, como smartphones e tablets, que no fundo também são computadores portáteis. Esses dispositivos frequentemente possuem serviço de GPS e, além disso, os celulares conectam-se automaticamente com a antena da célula mais próxima, o que revela em que célula encontra-se o telefone (e teoricamente o seu dono). A combinação dessas opções faz com que sejamos cada vez mais fisicamente rastreáveis.

Do ponto de vista da privacidade, essa situação seria semelhante a estar sendo constantemente perseguido por várias pessoas ao mesmo tempo. Se isso acontecesse na vida real, obviamente seria insuportável, mas a computação faz com que não sintamos isso da mesma maneira, ou com que simplesmente permaneçamos inconscientes dessa perseguição. A localização física de pessoas pode gerar preocupações de caráter moral, não menos sérias quanto aquelas já descritas na abordagem sobre o perfilamento em massa de usuários. Devemos mais uma vez sublinhar que os smartphones são, essencialmente, computadores muito potentes, com acesso à rede aberta, rede celular e serviço GPS praticamente contínuo, pois nós raramente desligamos os nossos dispositivos portáteis (nós os utilizamos e recargamos continuamente).

Os usuários comuns acham (antes de mais nada, pois são manipulados pelos marketeiros) que esta possibilidade de ser localizado é algo útil e, por isso, desejável. Pode-se receber ofertas de restaurantes, lojas e outros serviços (com um desconto excepcional, com certeza!), etc. perto de nós, mas deve-se considerar que o local onde estamos também pode falar o que estamos fazendo ou até o que estamos pensando ou crendo.

Imaginemos que o nosso telefone, plenamente rastreável, encontra-se em igreja, sinagoga ou mesquita, clinica que efetua abortos, clinica para portadores do HIV, área de uma manifestação antigovernamental, clube de gays, boate, sede de um partido ou organização, biblioteca temática, loja de armas, lugar onde foi cometido um crime (e nós obviamente não o cometemos) e assim por diante. O que isso pode significar para quem tenha interesse em verificar o log de localizações do nosso telefone? Nós podemos nos encontrar nestes lugares acompanhando uma outra pessoa. É possível verificar quem (melhor dizer, cujo dispositivo) estava na nossa proximidade em um momento dado.

A estes fatos devemos juntar as tecnologias de reconhecimento facial, de voz, de padrões de locomoção (*gait recognition*), entre outras. Agregando estes dados com os outros contidos em nossos telefones modernos (conversas, mensagens, acesso às redes sociais, sites de busca, etc.) e outras informações que existem em profusão, pode-se facilmente (na realidade, quase que instantaneamente) reconstruir toda a nossa vida social, inclusive os elementos mais íntimos dela, no que tange ao pessoal, segundo por segundo.

Os smartphones e toda a categoria de dispositivos chamados de "smarts" são mais um "eufemismo digital" elaborado com intuito neurolinguístico por estratégias de marketing. Os donos destas tecnologias são evidentemente mais "smart" do que os produtos e serviços assim

chamados, e, parece frequentemente, do que os consumidores deles.

3.9. Comunicação VoIP

Com a progressiva convergência digital, internet serve hoje cada vez mais também para efetuar conversas telefônicas. A vigilância desse modo de comunicação sempre esteve presente nas questões legais referentes à privacidade. A voz sobre IP não criptografada sofre das mesmas vulnerabilidades de qualquer outro tipo de comunicação por protocolos da internet (*sniffing*, etc.). O pior é que os serviços de VoIP, explorando a novidade dessa comunicação no plano normativo, são geralmente prestados por meio de contratos de licença em que o usuário abre voluntariamente mão da sua privacidade em favor do provedor do serviço, como o serviço Skype, por exemplo. Pagando pelo Skype por meio de conta bancária pela internet, nós nos identificamos. O Skype foi adquirido pela Microsoft por 8,5 bilhões de dólares em maio de 2011. A atuação dessa empresa no mercado mundial pode gerar muitos receios relacionados à privacidade dos usuários. Essa aquisição do Skype só os aumenta[83]. A Microsoft mudou as regras de criptografia e uso secundário de dados transmitidos entre os usuários e o servidores. A empresa efetivamente pode decodificar e ler todas as mensagens e ainda fornecer estes dados às organizações de segurança estatal[84]. Cabe ressaltar, que as grandes corporações tendem a cooperar com as autoridades estatais (de seus próprios países e, também, de estrangeiros), pois a desobediência poderia danificar seus negócios. Um exemplo muito famoso disso foi o acordo entre o Google e o Governo da China[85].

Cabe ressaltar que conversas telefônicas por meio da rede aberta, via de regra, encontram-se sob o mesmo domínio normativo que permite com que sejam grampeadas em certas situações. Quando elas não podem ser grampeadas ou o fato de serem muito mais baratas do que as telefonias fixa tradicional e móvel, provoca danos financeiros a grandes jogadores do mercado, podendo ocorrer o que se passou na Rússia – o Skype (também Gmail e Hotmail) foi declarado pelo Serviço Federal de Segurança como uma ameaça à segurança nacional e foi combatido pela União Russa de Industrialistas e Empresários[86]. A situação se normalizou em seguida, mas o FSB (Serviço Federal de Segurança da Rússia) pode vigiar a comunicação pelo Skype mesmo sem autorização judicial[87].

No caso da telefonia pela rede aberta, as preocupações referentes à privacidade são essencialmente as mesmas que surgem da utilização das redes de telefonia fixa e móvel: grampos, gravações de conversas, sua análise (inclusive com ferramentas informáticas para reconhecimento automático de voz) e intromissão no processo de comunicação (envolvendo a sua proibição ou bloqueio, por exemplo).

3.10. Computação em nuvem

A computação em nuvem tem o nome eufemístico que tem o poder neurolinguístico de disfarçar certas características do seu serviço. A palavra "nuvem" provoca associações com

83 Peter Bright, Microsoft Buys Skype for $8.5 Billion. Why, Exactly?, no site Wired, 10 de maio de 2011. http://www.wired.com/business/2011/05/microsoft-buys-skype-2/ (carregado em 18 de junho de 2013).

84 Dan Godin, ArsTechnica, Think your Skype messages get end-to-end encryption? Think again. 20 de maio de 2013. http://arstechnica.com/security/2013/05/think-your-skype-messages-get-end-to-end-encryption-think-again/ (carregado em 18 de junho de 2013).

85 Wikipédia inglesa, artigo "Google China", http://en.wikipedia.org/wiki/Google_China (carregado em 18 de junho de 2013).

86 The Telegraf, "Russian security service wants to ban Skype and Gmail" de 8 de abril de 2011. http://www.telegraph.co.uk/news/worldnews/europe/russia/8438617/Russian-security-service-wants-to-ban-Skype-and-Gmail.html (carregado em 18 de junho de 2013).

87 Thomas Nilsen, Barents Observer, "FSB can tap your Skype without court order", de 14 de março de 2013. http://barentsobserver.com/en/security/2013/03/fsb-can-tap-your-skype-without-court-order-14-03 (carregado em 18 de junho de 2013).

algo azul, celestial, distante e é "pré-formado" como algo bom. A computação em nuvem implica na virtualização do computador pessoal juntamente com todos os seus dados, que o usuário entrega voluntariamente a um terceiro ou terceiros. Em vez de guardar arquivos no computador local, o usuário os guarda na rede e, então, fica sem saber sobre a sua localização física, informação esta que o provedor do serviço não revela. A essa ideia, dá-se esse nome perigosamente simbólico.

As vantagens são as de poder acessar dados de qualquer lugar onde haja acesso à rede aberta e de não possuir aplicativos de importância básica (como pacote de escritório, por exemplo), o que no final das contas barateia custos.

Todos os riscos descritos até agora, que têm a ver com a possibilidade de revelação de dados pessoais ou de estes serem vazados ou bloqueados, devem aqui ser desconsiderados como riscos para o usuário desse tipo serviço, já que ele está consciente e voluntariamente entregando seus dados a um terceiro. A segurança "dos dados", seja lá o que isso signifique, e que normalmente é "assegurada" pelos provedores da computação em nuvem, é praticamente inverificável, e a probabilidade de uso secundário deles é muito alta. Com certeza, certos tipos de dado, como os médicos, não devem ou não podem ser entregues a nuvens. Os aspectos fundamentais da segurança de usuários relativa a dados em nuvem estão no foco de numerosas discussões hoje em dia[88].

3.11. Computação ubíqua

Computação ubíqua ou computação difusa (*ubiquitous computing*, *ubicomp*, *pervasive computing* ou *ambient intelligence*, em inglês) é o nome dado a um modelo de interação dos humanos com dispositivos digitais em vários âmbitos da vida cotidiana. Isso envolve o uso de dispositivos móveis, como celulares e computadores portáteis, interconectados com redes sem fio. Esse conceito estende-se, também, ao uso de dispositivos cuja presença ou regras de funcionamento (como de processadores em aparelhos domésticos modernos) não são obrigatoriamente de conhecimento do usuário. O objetivo geral da computação difusiva é permitir que aparelhos e dispositivos se reconheçam e comuniquem-se, ajudando, pelo menos em teoria, a melhorar os serviços prestados por eles aos usuários. Essa ideia foi proposta por volta de 1988 por Mark Weiser, na época um empregado da Xerox Palo Alto Research Center (PARC). Weiser definiu três categorias de dispositivos, com base nas dimensões de suas telas: tabs – dispositivos que podem ser levados no bolso, medindo alguns centímetros; pads – dispositivos que cabem na palma da mão ou possuem até alguns decímetros; e boards – aparelhos cujo tamanho é medido em metros. Logo, devido aos avanços tecnológicos, essa classificação foi enriquecida em mais três categorias: dust, skin e clay, que denominam os dispositivos ainda mais miniaturizados.

O problema relativo à privacidade com essa nova categoria de computação está na falta de consciência das pessoas a respeito de sua presença e na falta de conhecimento de suas regras de funcionamento.

3.12. Marketing individualizado e *Ad serving*

O marketing individualizado (*one-to-one marketing, relationship marketing*) não é algo totalmente novo na época digital. Ele já tinha surgido antes, mas só a tecnologia digital trouxe métodos e recursos para a sua ampla aplicação (quando surgiu um novo nome para ele – internet marketing). Essa modalidade de marketing gerou a moda de implementar em massa os sistemas CRM (gerenciamento de relacionamento com o cliente) e parece ser o combustível do mais novo negócio de dados pessoais.

No fundo, o Marketing, tanto o "tradicional" como o "digital" é uma mistura de boas

88 Uma análise bem completa das questões relativas à privacidade em nuvem pode ser encontrada em "Cloud Security and Privacy", Tim Mather, Subra Kumaraswamy, and Shahed Latif, O'Reilly, 2009.

práticas, convicções, psicologia, artes plásticas e cênicas, estatística e, hoje, informática, bem como vários outros domínios que são utilizados para aumentar a probabilidade de os consumidores adquirirem produtos ou serviços. O Marketing é um certo tipo de "alquimia moderna", sobre a qual não faltam as opiniões criticas[89]. Ele é profundamente interligado com o fenômeno de consumerismo, que também tem muitos oponentes (a Igreja Católica, entre outros). Devemos sublinhar que, tanto faz, sendo ele positivo ou negativo, ele está presente na nossa vida e é possível graças a riqueza material crescente das nações mais desenvolvidas. "A maioria dos homens vivem vidas de silencioso desespero", como proclamou Henry David Thoreau. O, que nós, representantes do mundo do capitalismo e da democracia, achamos de ser uma violação da nossa privacidade, ou até à nossa liberdade civil, é considerado um "paraíso na terra" por grande parte dos humanos que habitam o globo. Assim, os temas abordados na presente monografia (inclusive o marketing) são por natureza elitistas, oriundos de nações ricas.

A internet abriu mais um caminho para o desenvolvimento do marketing. A grande quantidade de dados sobre os usuários e o desenvolvimento da informática permitiram a criação de bancos de dados e o processamento desses dados para a elaboração de perfis de usuários consumidores. O marketing que trabalhou com grupos-alvo demográficos e psicográficos está rapidamente migrando para o marketing individual, em que se pode trabalhar com indivíduos bem identificados dentro desses grupos-alvo. Marcella e Stucky escrevem:

A crescente prevalência da internet e o surgimento do e-comércio levaram a um boom massivo na coleção de dados nos últimos anos. As empresas estão freneticamente acoplando bancos extensivos de dados, às vezes clandestinamente, na tentativa de realizar a utopia do relacionamento mais próximo com o cliente e do marketing individualizado (one-to-one marketing)[90] [tradução do autor]. Craig e Ludloff intitularam o capítulo dedicado a essa questão de *"A propaganda como um grande lobo malvado"*.[91]

O mundo dos negócios é um jogo de alto risco. Observar e prever os movimentos dos oponentes (da concorrência) tornou-se obrigatório, e reagir a eles o quanto antes se tornou indispensável. Assim, qualquer acontecimento novo no mercado, um novo lance, seja tecnológico, na comunicação publicitária ou de qualquer outro tipo, imediatamente se depara com a reação de todos os jogadores. Desse modo, as invenções nos negócios, mesmo nos não verificados, que apenas parecem promissores, espalham-se pelo mundo todo instantaneamente. É importante ressaltar que esse esquema tornou-se viável porque a economia e a indústria modernas já proveem bastantes recursos para financiar esse "jogo".

Mas por que a ideia do marketing individualizado seria ruim, ou até utópica? O *Permission Marketing*, descrito por Seth Godin no livro sob mesmo título[92], baseia-se no gerenciamento do relacionamento com o cliente individualizado que visa à construção gradual da confiança do cliente, sempre com o consentimento ou permissão deste à empresa. No fundo, essa ideia é boa, mas é de se imaginar que todo o mundo comercial se interessaria em adotar esse padrão de marketing? Na realidade, o elemento da permissão do consumidor não é apreciado pela maioria das empresas atualmente. No mundo dominado pelo marketing de permissão, receberíamos milhares de e-mails de spam todo dia (muito mais do que recebemos hoje), o nosso telefone não pararia de tocar, nas caixas de correio tradicionais teríamos pilhas enormes de ofertas. O marketing tradicional já se tornou suficientemente irritante e sua nova variação individualizada ainda multiplica esta impressão. Os consumidores não parecem ficar

89 "Criticism of advertising", Wikipédia inglesa, http://en.wikipedia.org/wiki/Criticism_of_advertising (carregado em 1 de julho de 2013).

90 Albert Marcella Jr., Carol Stucki, "Privacy Handbook, Guidelines, Exposures, Policy Implementation, and International Issues", p. 57.

91 Terence Craig e Mary E. Ludloff, "Privacy and Big Data", p. 5.

92 Godin Seth. "Permission Marketing: turning strangers into friends, and friends into customers", de 1999.

felizes neste relacionamento próximo corporação – consumidor:

Quando falamos com pessoas sobre suas vidas como consumidores, não ouvimos elogios para com os seus assim chamados parceiros corporativos. Em vez disso, ouvimos sobre um mercado confuso, estressante, insensível e manipulativo, em que eles se sentem pegos e vitimizados[93] [tradução do autor].

O marketing individualizado, em sua fase madura, faria de nossa vida um horror insuportável. O resultado disso poderia ser a fuga dos consumidores desses relacionamentos e perdas gigantescas por parte da indústria. Mas a indústria parece não se preocupar com essa visão. As empresas do mundo todo continuam construindo bancos enormes de dados a respeito dos consumidores. Porém, devemos ressaltar que há exemplos positivos na indústria e no setor público. Várias entidades demonstram certa preocupação com questões de privacidade dos usuários. Elas colocam em seus sites informações sobre a política de privacidade, partindo da premissa correta de que violações à privacidade do usuário podem comprometer sua imagem ou a condição comercial das marcas por elas oferecidas. Mas o quadro geral nessa área continua gerando muitas preocupações.

Uma pesquisa de 2009 demonstrou[94] que 66% de americanos adultos não querem os anúncios individualizados pré-preparados por marketeiros. Quando os pesquisados foram informados sobre os métodos de coleta de dados sobre eles, esta percentagem ainda cresceu, atingindo 73%-86%. Também, a maioria (55%) dos jovens (de 18 a 24 anos) demonstraram a mesma insatisfação.

Recapitulando, o propulsor do marketing individualizado não é só o dinheiro. Existe a forte crença na necessidade absoluta do seu desenvolvimento, o que resulta na elaboração de ferramentas informáticas que acabam por ameaçar ou invadir nossa privacidade e liberdade.

Os bancos de dados sobre os usuários podem não estar adequadamente protegidos e serem, consequentemente, desviados e utilizados contra os usuários. Surge então uma pergunta interessante. Será possível construir um banco de dados sobre todos os usuários da rede? Teoricamente sim, e parece que o Google tende a atingir esse alvo.

Mais uma preocupação vem do fato de os dados colecionados sobre os usuários não serem necessariamente verdadeiros, atuais, ou mesmo de desejável revelação por parte daqueles a quem se referem. A possibilidade de os usuários corrigirem ou mesmo verificarem esses dados é mínima. Assim, chegamos a uma conclusão muito séria – a tecnologia moderna, a internet em particular, tem grande potencial de mentir a nosso respeito. Do outro lado, para nos proteger na rede ou para construir a nossa "imagem digital", o que tem se tornado cada vez mais importante (sobretudo frente aos empregadores) é fornecer informações falsas sobre nós, o que significa dizer que essa mesma tecnologia nos permite e até nos “força” a mentir. De certo modo, ao nos fazermos presentes na rede, desejamos vestir as máscaras por nós escolhidas de acordo com a situação em questão. Isso simboliza a já citada liberdade de gerenciar separadamente nossos papéis sociais, pela qual, como já argumentado, a nossa privacidade se manifesta. Assim, a impossibilidade de influir nas nossas imagens virtuais na rede constitui violação aguda à nossa privacidade. Desejar corrigir ou deletar a nossa "imagem virtual", ou evitar que distintas imagens virtuais nossas se “misturem”, está fora do nosso alcance no tempo e no espaço, e assim, ficamos sem chance de agir neste sentido.

As empresas de marketing individualizado utilizam muitas das tecnologias supramencionadas para aumentar a probabilidade de compras, especialmente o *web tracking* (utilizando web bugs e cookies, entre outras técnicas), agregação e análise de dados e

93 Susan Fournier, Susan Dobscha, David Glen Mick, "Preventing the Premature Death of Relationship Marketing", Harvard Business Review, janeiro-fevereiro de 1998, p. 48.

94 Turow, Joseph, King, Jennifer, Hoofnagle, Chris Jay, Bleakley, Amy and Hennessy, Michael, Americans Reject Tailored Advertising and Three Activities that Enable It (September 29, 2009). Available at SSRN: http://ssrn.com/abstract=1478214 or http://dx.doi.org/10.2139/ssrn.1478214 (carregados em 3 de julho de 2013).

perfilamento de usuários. Eles também trocam e comercializam os dados sobre usuários, os quais, na área de marketing, servem para elaboração de sistemas automáticos de colocação de *ad serving*.

Ad serving é uma tecnologia de colocação de propagandas em páginas www. As empresas desta área disponibilizam aos donos de serviços www na rede e aos anunciantes (agências de publicidade e clientes diretos) os softwares que servem para colocação de anúncios, otimização da escolha de sites e usuários-destinatários, contagem de contatos dos usuários com anúncios, monitoramento de campanhas publicitárias, geração de relatórios e estatísticas, etc. O sistema informático para efetuar essas atividades chama-se adserver (abreviação de *advertisement server*, em inglês). As suas funções mais comuns são:

- manter o acervo de materiais de propaganda (banners, vídeos, animações, etc.);
- carregar os conteúdos de propaganda ao navegador do usuário;
- efetuar *targeting* de anúncios para usuários (escolha de propagandas para usuários previamente perfilados);
- efetuar *targeting* de anúncios conforme o contexto da página;
- gerar relatórios e coleta de estatísticas.

Os servidores podem também oferecer funcionalidades mais avançadas, como:

- *Frequency capping* (número de exibições de propagandas aos usuários é predefinido);
- Sequencionamento de exibições (o usuários recebem as propagandas na ordem predefinida);
- *Behaviour Targeting* – (direcionamento de anúncios conforme as atividades anteriores efetuadas por internautas).[95]

Um aspecto de se efetuar essas novas modalidades de marketing e publicidade permanece obscuro, como já foi na época do marketing pré-digital: por que o fato de se carregar algum conteúdo é tratado como equivalente à sua leitura ou observação, ou ainda, por que isso deveria significar que o usuário tenha se interessado de alguma forma por esse conteúdo, em particular por aqueles relativos a comunicações de propaganda? A inverificabilidade dessa hipótese na prática cria mitos sobre a eficiência da propaganda na internet e da propaganda em si. Esse mito remonta à época anterior, a da televisão, do rádio, da imprensa e de outros veículos de propaganda não-digital, e na internet alimenta também uma indústria da fraude em estatísticas sobre publicidade. A base de todas as pesquisas sobre a eficiência da propaganda está na descoberta do fato de ter ou de não ter havido o contato com a mensagem, e na correta contabilização desses fatos, também usada para precificar os serviços de *ad serving*.

No marketing de internet existe uma "medida do interesse" do consumidor – o "click" e o modelo de negócio baseando nesta medida é o "pay-per-click". Quando se clica em um anúncio em uma página web, o dono desta página recebe, através do sistema de *ad serving*, certa remuneração. Como é fácil de prever, existem sujeitos que escrevem programas que clicam nestes anúncios automaticamente para aumentar os ganhos financeiros. Eles chamam-se "clicadores falsos" ou "obsessivos"[96]. Eles prejudicam os investimentos feitos na rede aberta e contribuem à já sinalizada mitologização da eficácia da publicidade na rede aberta.

O marketing tradicional, este baseado em demografia ou até psicografia, dedica-se a criação de posturas e emoções em consumidores, mas o marketing individual vai ainda mais longe. Ele invade a esfera de emoções humanas com intuito de lê-las ou prevê-las. Estas não

95 Wikipédia inglesa, artigo "Ad serving", https://en.wikipedia.org/wiki/Ad_serving (carregado em 1 de julho de 2013).

96 Ferry Kate, Ad News, "Anúncio falso no Facebook comprova eficácia da rede social" http://www.adnews.com.br/publicidade/anuncio-falso-no-facebook-comprova-eficacia-da-rede-social (carregado em 1 de julho de 2013).

podem, ou não devem, ser "calculadas". Se forem, nós nos privaremos da nossa condição humana e ficaremos induzidos a meros artefatos comerciais.

3.13. Motores de busca

Existem vários motores de busca na rede aberta, mas os usuários comuns tendem a associar o acervo da rede com os serviços prestados pelo Google ou, já muito mais raramente, com a Yahoo ou outras empresas do mesmo tipo. Por motivos óbvios, vamos nos concentrar no Google mesmo.

O Google é uma empresa que aparece mais frequentemente na mídia, mais frequentemente nas disputas com os órgãos de administração e de legislação e, em geral, está constantemente no foco deste assunto candente. Os motivos deste interesse são numerosos, e nem sempre diretamente compreensíveis pelos usuários comuns.

O Google, graças ao seu modelo único de negócio na rede aberta, conseguiu verdadeiramente conquistá-la e dominá-la em escala global, e isto aconteceu muito rapidamente. Este modelo foi, inicialmente, de concentrar-se no fornecimento de resultados de busca o mais rápido possível e evitar de sobrecarregar os usuários com propagandas (isto, a propósito, confirma que o marketing tradicional é algo ruim, também do ponto de vista da maior empresa de marketing do mundo). Enquanto seus concorrentes, como Altavista e Yahoo, bombardeavam os usuários com propagandas lucrativas na sua página inicial, o Google presentava uma página muito modesta, até ascética, devolvendo resultados esperados muito mais rapidamente do que a concorrência e sem nenhuma propaganda. Logo, quase todo mundo mudou para o serviço do Google. As empresas como Altavista e Yahoo não compreenderam e continuam a não compreender como funciona a psique dos consumidores (dos humanos, afinal de contas) e de como funciona a vida de uma marca comercial. O efeito disso é uma perda espetacular da *market share* e, como a história demonstra, nem Seth Godin, um dos diretores da Yahoo, com suas teorias de *Permission Marketing*, conseguiu consertar este desbalanço.

O Google, já faz tempo, não é apenas um motor de busca, embora esta atividade permaneça a mais importante no negócio desta empresa. Atualmente o Google oferece dezenas de serviços e muitos deles causam ansiedades em relação à privacidade de usuários[97]. Além disso, a mesma mentalidade do negócio desta empresa causa ansiedades e a coloca na frente do Colonialismo Eletrônico[98] (com certeza junto com o Facebook[99]). As críticas em relação ao Google já foram catalogadas separadamente na Wikipédia[100]. Nós vamos indicar os fatores mais gerais ligados à atividade desta empresa.

Antes de mais nada, como também no caso do Facebook, o problema principal é o alcance global de suas atividades, dinheiro a sua disposição e agressividade extrema do negócio privado, sobre quaisquer reflexões de natureza referente à privacidade. Reppesgaard convoca dois acontecimentos interessantes:

Em 2005, uma jornalista, Elinor Mills, preparava uma publicação sobre o Google. Graças ao que encontrou através do Google mesmo, chegou a saber que o Eric Schidt morava com sua esposa em Atherton, na California, dispunha de riqueza de 1,5 bilhões de dólares e um ano atrás tinha adquirido as ações no valor de 140 milhões de dólares. Ela informou, também, que Schmidt gostava de pilotar aviões e recentemente tinha participado no Festival do

97 Wikipédia, artigo "List of Google products" http://en.wikipedia.org/wiki/List_of_Google_services_and_tools (carregado em 1 de julho de 2013).

98 Wikipédia, artigo "Electronic colonialism", http://en.wikipedia.org/wiki/Electronic_colonialism (carregado em 1 de julho de 2013).

99 Dan Farber, "Facebook Colonizing the Internet", CBS News, http://www.cbsnews.com/8301-501465_162-20023480-501465.html (carregado em 1 de julho de 2013).

100 Wikipédia, artigo "Criticism of Google", https://en.wikipedia.org/wiki/Criticism_of_Google (carregado em 1 de julho de 2013).

Homem Ardente (Burning Man Festival). Os Googlers ficaram com grande rancor – estas informações ameaçavam a segurança do seu diretor de finanças! Durante um ano a seguir, eles evitaram os jornalistas do empregador da Mills, a empresa Cnet.[101] [tradução do autor].
Depois do lançamento do projeto Google Street View, os jornalistas do "The Australian" efetuaram um experimento:
Eles pediram aos funcionários importantes no Google que fornecessem seus endereços residenciais para que os repórteres pudessem fazer fotos de suas casas, necessárias para um artigo a ser publicado. O Google recusou. O seu porta-voz disse que isso seria inaceitável. A conclusão dos repórteres australianos foi a seguinte: "As pessoas governando o sistema ávido do Google passam seu tempo desenvolvendo as tecnologias que derrubam a privacidade do indivíduo, mas quando têm que revelar os seus próprios dados pessoais, ficam extremamente relutantes em colaborar."[102] [tradução do autor].

O Google oferce, entre outros, o maior serviço de busca, serviço de e-mail, de rede social (Google+, Orkut), de armazenamento de fotos (Picassa Web Albums), de registros médicos (Google Health), de telefonia (Google Phone, baseado no sistema Android), de calendário de eventos e compromissos (Google Calendar), de perfilamento de usuários (Google Profile), de vídeo (You Tube), de localização geográfica (Google Maps, Google Earth, Google Street View), de contatos com outras pessoas (Google Hangouts), de armazenamento de documentos em nuvem (Google Docs), etc. Em 2012 o lucro do Google foi de 50 bilhões de dólares[103]. Todos estes fatos confirmam que estamos enfrentando um excesso gigantesco de poder. O Google sabe sobre nós muito mais do que qualquer governo ou empresa neste mundo.

Atualmente, o mundo espera o lançamento do Google Glass, um computador portátil em forma de óculos que permite, entre outras opções, a gravação de áudio e vídeo. Isso já causa várias preocupações morais e éticas, como por exemplo, tais gravação poderem ser efetuadas sem permissão de pessoas.

3.14. Redes sociais

As redes sociais virtuais tornaram-se extremamente populares nos últimos anos. Elas funcionam oferecendo uma plataforma que permite ao usuário manter contatos interpessoais, fazer listas de amigos, informá-los sobre o seu perfil, ver os perfis deles, colocar fotos e vídeos e também acessar várias aplicações, como *chat,* jogos, *blogs*, entre outras. A maior rede social virtual hoje é o Facebook, fundado em 2004. Segundo dados próprios[104], em maio de 2013 o Facebook contava com 751 milhões de usuários. A metade acessa o serviço por meio de dispositivos móveis, que, como já sublinhamos, trazem muito mais preocupações sobre a privacidade e liberdade de usuários do que os computadores tradicionais.

A identidade de usuários reais, tão procurada por empresas e agências estatais de segurança na internet e fora dele, é tão facilmente encontrada nas redes sociais virtuais. Além de dados como nome, sobrenome, e-mail, sexo e idade, por exemplo, que o Facebook solicita aos novos usuários, estes frequentemente colocam em seus perfis muitas outras informações de caráter privado (fotos, contatos, números de telefones, localização, pensamentos, opiniões, interesses, compras, etc.). Existem suposições sérias de que essa prática possa favorecer a criminalidade virtual, em particular os abusos sexuais. Os integrantes dessas comunidades frequentemente não estão conscientes das ameaças oriundas da internet. Um dos problemas está no controle de dados nesses *sites*, pois dados modificados ou deletados podem ser

101 Lars Reppesgaard, "Imperium Google" (título original: "Das Google-Imeprium", de 2008), edicação polonesa de 2009, p. 109.
102 Ibid. p. 149.
103 http://investor.google.com/earnings/2012/Q4_google_earnings.html
104 https://newsroom.fb.com/Key-Facts

restituídos e cair nas mãos de outras pessoas. O acesso ao *site* por dispositivos móveis faz com que o fluxo de dados passe pelos provedores de telefonia celular. As redes sociais virtuais colaboram com empresas que fornecem dados adicionais sobre os usuários, agregando esses dados para realizar *targeting* de publicidade e vender campanhas de propaganda.

As redes sociais virtuais ilustram uma desistência em massa da intenção de proteger a própria privacidade, embora seja injusto afirmar que seus usuários não reagem a certas ações invasoras por parte dos donos desses sites, ou que não têm quaisquer expectativas em relação à proteção de seus dados dentro desses serviços.

O modelo de negócio de sites de redes sociais remete ao de igrejas: ganhar dinheiro ao juntar pessoas e fornecer a elas a sensação mais ou menos ilusória de estarem em comunidade (que tendemos a perceber como algo unificador, que fornece o sentimento de segurança, abrigo e amizade). É por isso que a contraposição dos donos dos sites de redes sociais em relação aos seus usuários, no que diz respeito aos aspectos de proteção à privacidade, soa tão injusta e imoral. Do lado do invasor, há simplesmente a vontade induzida pela lógica de mercado de reconstruir virtualmente a identidade mais completa possível dos usuários para ganhar dinheiro. Não existem aqui sentimentos humanos que se associem ao direito ou desejo de privacidade dos usuários. Estes constituem apenas registros em bancos de dados. Se a privacidade deles é declarada como estando protegida, isso serve apenas para manter o negócio; ou seja, ela é declarada e só isso. Do outro lado, estão os usuários leigos e ingênuos, privados da possibilidade de se defender ou de fiscalizar tais declarações, mas, paralelamente a isso, também portadores de um desejo humano antagônico e potente de se socializarem. Entre essas duas partes do negócio, encontra-se a silenciosa, intocável e intermediadora *esfera da computação*, controlada pelo invasor. Ela esconde, falsifica ou disfarça o fator de invasão e engana os nossos instintos de proteção. Ela também fornece amparo aos nossos instintos de socialização, o que ocasiona decadência geral das relações íntimas, que habitam o cerne do conceito de privacidade. A tecnologia enfraquece os já fracos laços emocionais nas sociedades modernas.

Há mais fatos observáveis que podem fazer prova da tese supramencionada.

A instituição da confissão no Facebook e outros sites de redes sociais é *presumida*. No Facebook existe uma opção de votar por algo que se gosta (*I like this*, ou “curtir”), mas não existe nenhuma opção de votar contra, com um click em "Não gosto", mas por que? É óbvio que os donos do negócio não querem brigas e, em consequência, cismas na organização do seu negócio.

As redes sociais tendem a atrair os novos membros, obviamente com o intuito de retirá-los de outros sites semelhantes. Temos aqui um exemplo do proselitismo, algo tão ardente na discussão dificílima sobre ecumenismo, no mundo real. No mundo de negócios não há, nem nunca haverá, nenhum sinal do "ecumenismo comercial".

Falando com os membros de sites de redes sociais sobre os riscos à privacidade e até à liberdade, frequentemente enfrentamos reações semelhantes àquelas que surgem quando temos ousadia de criticar a política de comunidades religiosas no mundo real. Os interlocutores, via de regra, reagem com grande nervosismo e até hostilidade, como em uma situação de alguém tentando erradicar suas raízes morais, suas tradições, valores oriundos da educação obtida na infância, a memória e estima de seus ancestrais, etc.

Os membros de sites de redes sociais mais populares tratam os que não participam neles como "ateus", e os ostracizam.

O fator equivalente ao de prometer a vida eterna, que muitas religiões colocam no primeiro lugar, também está presente nas redes sociais. Não é que, colocando as informações detalhadas sobre quase cada momento da nossa vida, mostrando-nos como pessoas melhores do que somos ou estamos (as fotos nossas dos tempos da juventude, em vez das atuais) nós tentamos de certo modo a nos eternizar?

As redes sociais virtuais estão na moda. Elas implantam modelos de comportamento, incluindo o de descuido com aquilo que é privado. Temos aqui um exemplo de retroalimentação da decadência do valor atribuído pelos usuários desses serviços à privacidade. Privacidade é mercadoria, cada vez mais barata. Quando ocorre descuido generalizado com relação a ela, causa-se a erosão do preço desse bem, já não mais apenas simbólico mas também plenamente real.

Os sites sociais podem servir, também, para perseguição, difamação, assédio, destruição de reputação, etc., e também de forma coletiva (várias pessoas perseguindo uma vítima). As vítimas são frequentemente mulheres, menores de idade, minorias sexuais. Estas invasões receberam o nome de *cyberbullying, cyberstalking* e *cyberharrasment*. O *cyberbullying* é comumente percebido como efetuado por menores de idade e direcionado a menores de idade (mas na verdade não é limitado a estes casos), enquanto o *cyberstalking* e *cyberharrasment* referem-se aos casos de ações hostis de adultos contra adultos. Devemos recordar os casos dos suicídios de jovens que sofreram abusos nas redes sociais: Megan Meier[105], Tyler Clementi[106], Amanda Todd[107], Phoebe Prince[108], Ryan Halligan[109].

3.15. Empresas de alocação de emprego e recrutamento

Entre as empresas que colecionam e comercializam dados sobre os usuários da rede aberta, destacam-se, de uma maneira potencialmente muito perigosa, as empresas de alocação de emprego e recrutamento. A internet tornou-se a principal fonte de oferta e procura de emprego. A imprensa ainda continua sendo veículo de anúncios de emprego, mas, na maioria dos casos, os mesmos anúncios também aparecem na internet. Ao se candidatarem a uma posição, os usuários devem fornecer não apenas seus dados pessoais para contato, mas também seu currículo, que costuma conter todos os pontos de sua trajetória profissional, bem como aspectos como interesses profissionais, detalhes da vida familiar, entre outros. O currículo é, em princípio, nosso mini perfil, que entregamos de graça às empresas intermediadoras. Além disso, se utilizamos serviços de e-mail "gratuitos", como o yahoo.com ou o gmail.com, nossos currículos também acabam caindo nas mãos dessas empresas.

3.16. Monitoramento de empregados

Os empregadores desejam monitorar a lealdade, moralidade e eficácia profissional de seus empregados observando suas ações ao utilizar o computador de trabalho, sua interação com a rede e também sua correspondência via e-mail e conversas telefônicas. Na pesquisa da AMA de 2007, dois terços de empregadores monitoram o uso da internet pelos seus empregados[110]. A vigilância pelas câmaras no lugar de trabalho também é muito popular. As pessoas que trabalham como motoristas podem ser rastreadas pelos dispositivos GPS. De novo, devemos sublinhar que a localização dos telefones celulares torna-se uma rotina e os

105 Megan Meier Foundation, http://meganmeierfoundation.org/megansStory.php (carregado em 23 de junho de 2013).

106 The Tyler Clementi Foundation, http://www.tylerclementi.org/tylers-story/ (carregado em 23 de junho de 2013).

107 Christina Ng, ABC News, "Bullied Teen Amanda Todd's Death Under Investigation", http://abcnews.go.com/US/bullied-teen-amanda-todds-death-investigation/story?id=17489034 (carregado em 23 de junho de 2013).

108 Russell Goldman, ABC News, "Teens Indicted After Allegedly Taunting Girl Who Hanged Herself", http://abcnews.go.com/Technology/TheLaw/teens-charged-bullying-mass-girl-kill/story?id=10231357#.UccNQcjLf9c (carregado em 23 de junho de 2013).

109 Ryan's story, http://www.ryanpatrickhalligan.org/about/about.htm (carregado em 23 de junho de 2013).

110 American Management Association, 2007 Electronic Monitoring & Surveillance Survey, http://press.amanet.org/press-releases/177/2007-electronic-monitoring-surveillance-survey/ (carregado em 22 de junho de 2013).

empregadores também podem utilizá-la. Os *tags* RFID em crachás servem para acessar várias áreas no lugar de trabalho e as passagens nas proximidades de um leitor de RFID podem ser gravadas em bancos de dados.

Os empregadores podem também requerer e manter os dados médicos sobre os seus empregados, efetuar testes psicológicos e outros ou até intencionalmente desafiar a corretude profissional de seus funcionários. Finalmente, os empregadores são destinatários dos nossos mini perfís em forma de CVs. Eles os podem armazenar, mesmo quando os empregados já não trabalham mais para eles. Em resultado, frequentemente os empregadores sabem muito mais sobre os seus empregados do que seria objetivamente necessário, neste contexto.

Em vários países do mundo, a defesa contra este tipo de monitoramento praticamente não existe ou é problemática, como nos EUA[111]. No Canada, o monitoramento de empregados é proibido, a menos que seja feito com conhecimento do empregado e quando isso é objetivamente necessário[112].

O monitoramento de empregados traz muitos problemas da natureza moral, tanto do ponto de vista dos interesses do empregadores, como direitos dos empregados. Com certeza, os empregadores têm direito de esperar que os seus empregados façam o seu trabalho de uma maneira adequada e eficiente. Eles têm que defender os dados referentes ao seu negócio contra vazamentos ou ataques internos e externos e, também, identificar as situações em que os recursos corporativos, como e-mail ou intranet, estejam sendo indevidamente utilizados, por exemplo para fazer piadas racistas, efetuar mobbing ou de qualquer outro modo prejudicar os interesses e a imagem da empresa. Os empregados, por seu lado, têm direito de não ser observados e monitorados de uma maneira não justificada e excessiva, mas, pelas mesmas razões morais, não devem passar o seu tempo no trabalho navegando a rede por motivos pessoais.

Outra observação é que os empregadores, em muitos casos, têm capacidades técnicas de efetuar vários tipos de vigilância de seus empregados, como o monitoramento de e-mails e o uso de internet em particular, mas se abstêm de fazer isso, pois isso poderia estragar o ambiente profissional, introduzir uma atmosfera de desconfiança e prejudicar as relações entre os empregados e o empregador, bem como entre os empregados mesmos. Isso nos parece o caminho mais adequado ou correto para tratar do assunto, mas, infelizmente, a realidade é diferente.

Existem muitos softwares para efetuar o monitoramento de empregados, por exemplo o já citado Spector, e todos eles pertencem à categoria de softwares de espionagem. Além do Spector, no mercado ainda funcionam: InterGuard, Employee Desktop Live Viewer, Network Enforcer, NetVizor, Spytech SpyAgent, Ascendant NFM, KeyGhost Keylogger, etc.[113]

3.17. Monitoramento por agências estatais

O monitoramento de Internet pelas agencias estatais é onipresente hoje em dia (entre vários outros tipos de vigilância). Este monitoramento frequentemente utiliza o já mencionado "princípio de carona", i.e., vinculado a fatores reais, ilusórios ou fabricados para justificar a vigilância de cidadãos em massa, mas temos também muitos exemplos de governos que não se preocupam em justificar suas ações. O monitoramento da rede pelos poderes estatais obviamente pode servir para descobrir ameaças de caráter criminal (terroristas, pedófilos e outros criminosos), mas também para perseguir oponentes políticos, detectar tentativas de

111 Privacy Rights Clearinghouse, https://www.privacyrights.org/fs/fs7-work.htm#gps (carregado em 2 de julho de 2013).

112 Office of the Privacy Commissioner of Canda, "Privacy in the Workplace", http://www.priv.gc.ca/resource/fs-fi/02_05_d_17_e.ASP (carregado em 2 de julho de 2013).

113 Staff Monitoring Solutions, http://www.staffmonitoring.com/P32/monitoring.htm (carregado em 2 de julho de 2013).

pessoas se organizarem[114], censurar conteúdos da web[115] ou fechar sites[116]. Em várias partes do globo, a Internet é uma ferramenta potente para sustentar regimes perversos.

A organização Reportes Without Borders publica anualmente os relatórios intitulados "Enemies of the Internet", nos quais descreve as atividades dos governos que se destacam particularmente de forma negativa, dividindo-os em dois grupos: "países sob vigilância" e "inimigos de internet". Em 2012, a lista incluiu os seguintes países (o fato de não aparecer nesta lista não significa que os demais países não efetuam vigilância da rede)[117]:

Tabela 1. Países sob vigilância e Inimigos de internet conforme os Reportes Without Borders, em 2012.

Países sob vigilância	Inimigos de internet
Austrália	Bahrein
Egito	Bielorrússia
Erítrea	Myanmar (Birmânia)
França	China
Índia	Cuba
Cazaquistão	Irão
Malásia	Coreia do Norte
Rússia	Arábia Saudita
Coreia do Sul	Síria
Sri Lanka	Turcomenistão
Tailândia	Uzbequistão
Tunísia	Vietnã
Turquia	
Emiratos Árabes Unidos	

As ações repressivas e violações de direitos humanos em países como China, Rússia e outros países pós-soviéticos até que não são surpreendentes, mas os anos recentes trouxeram novas notícias muito mais graves sobre os países comumente percebidos como democráticos e que supostamente preservam os conceitos da liberdade e cidadania. Falamos aqui sobre os posts do Wikileaks[118] (desde 2006) que se referem a muitos desses países, e às denúncias de Edward Snowden, ex-agente da CIA (em 2013) que se referem aos EUA[119].

Não vamos avaliar aqui os aspetos morais das revelações efetuadas por Julian Assange (Bradley Manning) e Edward Snowden, pois, talvez, seja cedo demais para fazer isso. Vamos apenas frisar que o resultado destas denúncias é a queda espetacular da imagem ideológica destes países, dos EUA e do Reino Unido em particular. Os EUA, comumente percebidos como uma oásis de liberdade, efetuam, já faz tempo, uma vigilância de todos os seus cidadãos e, também, dos estrangeiros e até no globo todo, em escala antes inimaginável. A situação não é melhor na Grã Bretanha.

---

114 Cabe recordar as ações da ABIN no Brasil em 2013 - Alana Rizzo e Tânia Monteiro - O Estado de S. Paulo, " Abin monta rede para monitorar internet", http://www.estadao.com.br/noticias/cidades,abin-monta-rede-para-monitorar-internet,1044500,0.htm (carregado em 3 de julho de 2013).

115 A China se destaca neste contexto: Wikipedia, artigo "Internet censorship in the People's Republic of China", http://en.wikipedia.org/wiki/Internet_censorship_in_the_People%27s_Republic_of_China (carregado em 3 de junho de 2013).

116 A Rússia utilizou a "carona" de proteção de menores para compor um lista de websites a serem fechados sem ordem judicial e sem direito à defesa, em novembro de 2012. Reportes Without Borders, "Internet Enemies Report 2012", http://march12.rsf.org/i/Report_EnemiesoftheInternet_2012.pdf (carregado em 3 de junho de 2013).

117 http://march12.rsf.org/i/Report_EnemiesoftheInternet_2012.pdf (carregado em 3 de junho de 2013).

118 wikileaks.org.

119 The Guardian e The Washington Post de 6 de junho de 2013. A transcrição da entrevista de Snowden para The Guardian pode ser encontrada a http://www.policymic.com/articles/47355/edward-snowden-interview-transcript-full-text-read-the-guardian-s-entire-interview-with-the-man-who-leaked-prism (carregado em 3 de julho de 2013).

Combatendo ideologicamente, desde o fim da Segunda Guerra Mundial, os sistemas opressivos comunistas na União Soviética e no seu bloco de países aliados (não voluntariamente aliados, porém), bem como na China, os EUA e seus aliados no mundo ocidental não previram um acontecimento muito particular – que esses seus inimigos políticos abrissem mão do controle da iniciativa privada na economia e que nestes países surgissem mercados mais ou menos livres. A corrida armamentista quase matou a economia da União Soviética. Os economistas e politólogos sinalizavam esta possibilidade antes dos Acordos da Mesa Redonda na Polônia, em 1989, com os quais começou o colapso da União Soviética. Do outro lado, não temos evidências de que este colapso da União Soviética e do seu sistema político no exterior fosse previsto pelos órgãos da inteligência dos EUA ou de que esta perspectiva fosse tratada como algo plausível[120].

De repente, para o mundo ocidental, os seus oponentes ideológicos viraram oponentes econômicos, e, como demonstram os resultados financeiros, eles rapidamente crescem como tal. O que acontece nos EUA parece demonstrar certa decadência, receio de perder a posição de liderança na economia mundial. Uma situação semelhante, na área tecnologica e militar, surgiu em 1957 quando os Russos lançaram o Sputnik, o que desencadeou o áuge do Macartismo, que chegou a dominar a vida política norte-americana nos anos 50. Os EUA estão perdendo a corrida econômica para com a China e isso parece ser inevitável e, ao mesmo tempo, impensável e inaceitável, para os círculos governamentais norte-americanos. Em consequência, os governos dos EUA, esquerdistas e direitistas (essa divisão parece ser um pouco artificial, considerando suas ações reais, tanto no interior como no exterior) imitam os sistemas e modelos de ações dos Estados que temem. O problema é aumentado pelo fato de os oponentes ainda não disporem de tecnologia tão forte. Logo, o mundo ocidental, ainda liderado pelos EUA, demonstra uma susceptibilidade às distorções antidemocráticas muito mais graves em relação à sua nova rivalidade econômica. Enquanto a Rússia e a China lentamente avançam na direção da democracia, pelo menos por meio da liberação das relações econômicas, os EUA e seus aliados destroem os princípios da democracia e liberdade em nome de uma segurança (mais ou menos ilusória), por onde definha a privacidade.

Ao mesmo tempo, a vigilância dos usuários da rede e dos cidadãos comuns pelos governos torna-se, cada vez mais, um negócio muito lucrativo. O relatório dos Reporters Without Borders do ano 2013 destaca isso em especial, pois dedica-se não apenas às violações dos direitos humanos no que diz respeito à censura da rede e a perseguição de jornalistas e ativistas, mas à vigilância da rede como tal e aos agentes comerciais que fornecem as ferramentas de hardware e software para efetuá-la em escala nacional, particularmente nos países com regimes claramente perversos. Eles são: Amesys, Blue Coat, Gamma International, Hacking Team e Trovicor[121].

Os estados dispõem de muitas vantagens na vigilância da rede aberta, em comparação com as entidades comerciais. Eles podem forçar os sujeitos normativamente subordinados: pessoas físicas, empresas provedoras de acesso à internet, grandes "jogadores" no mundo de negócios de dados pessoais, a revelar os seus acervos de dados ou dar acesso a estes ou à infraestrutura dos meios de comunicação. Eles também podem utilizar a infraestrutura militar para farejar as comunicações no nível de sinais eletromagnéticos.

Devemos frisar que, quando se trata de sistemas de vigilância construídos e controlados pelas agências de segurança pública, as informações atingindo o público são frequentemente incompletas, obscuras e as suas origens não são verificáveis. Os programas de vigilância estatal já existem em vários países e as notícias sobre os novos sistemas aparecem

120 Wikipedia inglesa, artigo "Predictions of Soviet collapse", http://en.wikipedia.org/wiki/Predictions_of_Soviet_collapse (carregado em 3 de julho de 2013).

121 Reporters Without Borders, "Enemies of the Internet 2013", http://surveillance.rsf.org/en/wp-content/uploads/sites/2/2013/03/enemies-of-the-internet_2013.pdf (carregado em 3 de julho de 2013).

na mídia com frequência. Vamos descrever dois sistemas dos EUA que são particularmente potentes: Echelon e PRISM.

Echelon

Logo depois da Segunda Guerra Mundial, em 1946, os EUA e o Reino Unido assinaram o acordo sigiloso denominado UKUSA (United Kingdom – United States of America Agreement) sobre a cooperação na área da inteligência através da interceptação de sinais de comunicações (SIGINT). A este tratado juntaram-se em seguida o Canada, a Australia e a Nova Zelândia (os membros principais da Comunidade de Nações) e surgiu o novo nome-código desta aliança: AUSCANNZUKUS (e também Five Eyes). Ele foi secreto e só em 2010 os documentos relacionados a ele foram desclassificados como secretos[122]. Os cinco signatários dividiram o globo em partes, nas quais que cada um foi responsável pela vigilância de sinais de comunicações. As partes trocavam estas informações entre si por motivos relacionados ao trabalho da inteligência. Com base neste acordo, foi construída uma rede de coleta e análise de dados que recebeu o nome de Echelon.

O sistema Echelon é uma rede de antenas parabólicas em várias partes do globo que interceptam os sinais de satélites para efetuar a vigilância de conversas telefônicas e de transmissões de dados. As provas de sua existência apareceram publicamente só em 1999. É óbvio que esta classe de ações pode ser considerada uma espionagem estatal e uma violação aguda de direitos humanos – algo que poderia causar danos enormes de caráter político, social e econômico. Por isso, já em 2000, a o Parlamento Europeu requereu aos EUA e ao Reino Unido que fornecessem explicações acerca da possível vigilância dos seus cidadãos por meio deste sistema. A resposta indicou que o alvo da vigilância pelo Echelon tinha, antes de mais nada, o caráter de espionagem industrial para descobrir fraudes e atos de corrupção. Em 2001, o Comitê Temporário do Parlamento Europeu publicou um relatório[123] no qual recomendou aos cidadãos dos estados membros criptografar suas comunicações para proteção da sua privacidade, pois o Echelon efetuando esta vigilância poderia comprometer (a vigilância poderia ser facilmente estendida para fora da área de espionagem industrial).

PRISM

O programa PRISM foi lançado em 2007 pela National Security Agency dos EUA. Ele foi altamente sigiloso. O mundo chegou a saber sobre sua existência em resultado das denúncias de Edward Snowden, ex-agente da CIA e funcionário terceirizado da NSA, em 2013[124]. Este programa prevê a possibilidade de monitoramento de todos os cidadãos norte-americanos na sua comunicação por telefones, e-mail, internet e por qualquer outro meio. No caso da internet e e-mail, este sistema pode de fato monitorar todos os usuários dos serrviços dos parceiros do programa, não somente os dos EUA.

Os documentos revelados por The Guardian enumeram várias empresas comercias que colaboram com NSA no programa PRISM: Microsoft, Yahoo, Facebook, Google, Apple, etc. Após a publicação, as empresas distanciaram-se destas afirmações[125].

---

122 NSA Press Release de 24 de junho de 2010, Declassified UKUSA Signals Intelligence Agreement Documents Available - http://www.nsa.gov/public_info/press_room/2010/ukusa.shtml (carregado em 20 de junho de 2013).

123 European Parliament, Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)) de 11 de julho de 2001, http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A5-2001-0264&language=ET (carregado em 20 de junho de 2013).

124 Glenn Greenwald, "Edward Snowden: the whistleblower behind the NSA surveillance revelations", http://www.guardian.co.uk/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (carregado em 20 de junho de 2013).

125 TechCrunch.com, "Google, Facebook, Dropbox, Yahoo, Microsoft, Paltalk, AOL And Apple Deny Participation In NSA PRISM Surveillance Program", http://techcrunch.com/2013/06/06/google-facebook-

Em 4 de junho de 2013, o Parlamento Europeu rejeitou a proposta dos Social-democratas e dos Verdes de adiar as negociações com os EUA sobre o comércio livre por causa do escândalo do PRISM, mas a Comissão Europeia vai efetuar uma investigação sobre a influência deste programa na liberdade e direitos dos cidadãos da UE e apresentar um relatório, antes do fim de 2013[126].

O sistema PRISM demonstra que o apetite dos EUA por dados dos usuários é insaciável e doentio e que os princípios democráticos neste país são, cada vez mais, uma ilusão. Os posts do Wikileaks e as revelações de Sonwden demonstram que os EUA não têm mais (e parece que de há muito não tem) os "princípios" que guiaram sua fundação – eles têm "interesses". Mas esta afirmação, justamente, não deve ser limitada só aos EUA, pois os serviços de inteligência do mundo todo vivem numa guerra interminável de todos contra todos, tal qual o "estado natural" de Hobbes, [cabe aqui citar a obra de Thomas Hobbes "Leviathan"] onde não há nenhuma aliança "verdadeira". Simplesmente, os serviços de inteligência, exércitos e diplomacias dos EUA e de seus aliados não tiveram sorte ao se verem vítimas de vazamentos de dados sigilosos. Isso não aconteceu por causa do trabalho clandestino de terroristas. Isso aconteceu por causa da postura de seus próprios cidadãos. Logo, o alvo principal da vigilância total não são terroristas (eles aparentemente sabem defender-se bem ou melhor do que os cidadãos comuns)[127], mas todos os cidadãos. Assim, todos somos tratados como possíveis criminosos.

3.18. Fraudes virtuais

3.18.1. Introdução

As fraudes cometidas com uso da rede aberta receberam o nome de fraudes virtuais, em português (internet frauds, em inglês). Infelizmente, este nome não é muito preciso. Seria mais adequado afirmar que o ambiente em que elas são cometidas é virtual. "Virtual" significa algo emulado, ou distante do real, enquanto estas fraudes são muito reais no sentido de suas consequências.

O alvo de invasões não é apenas a nossa privacidade, mas antes, a nossa propriedade, particularmente o nosso dinheiro (o caso do "roubo" de identidade é muito particular e por isso é descrito separadamente a seguir).

Nas fraudes eletrônicas podemos discernir dois tipos de ações: técnicas e não técnicas. O primeiro tipo são invasões com uso de tecnologia (hacking tecnológico). O segundo tipo são invasões com uso da manipulação psicológica de pessoas. As fraudes deste segundo tipo se baseiam em ganhar confiança de uma vítima para cometer estelionatos. As ações do invasor podem direcionar-se para uma ou mais qualidades do caráter humano, tanto positivas, como benevolência, altruísmo, empatia, como negativas: ganância, vaidade, etc. Na área da segurança da informação, as atividades não técnicas receberam o nome de Engenharia Social. Esta categorização não significa que os hackers não possam misturar essas modalidades de ataques. Os roteiros de ataques reais podem ser extremamente complexos. Como a prática demonstra, é frequentemente muito mais fácil conseguir os dados e informações sensíveis manipulando pessoas do que invadindo sistemas informáticos diretamente.

A manipulação de conteúdos das páginas web para enganar os usuários e obter os seus dados pessoais chama-se Phishing. Uma variação dele, que visa redirecionamento da requisições aos serviços na web, recebeu o nome de Pharming. Ambas estas invasões podem

---

apple-deny-participation-in-nsa-prism-program/ (carregado em 3 de julho de 2013).

126 BBS News, "Joint EU-US group to assess US spy ops", http://www.bbc.co.uk/news/world-europe-23165257 (carregado em 4 de julho de 2013).

127 O golpe em Boston aconteceu em 2013, i.é. muitos anos depois do lançamento do PRISM. O que realmente faltou no "sistema da vigilância total" para descobrir os planos dos terroristas e prevenir as mortes de pessoas inocentes?

levar ao furto de identidade de um usuário.

3.18.2. Furto de identidade

Esse tipo de conduta, chamada no direito brasileiro "falsidade ideológica"[128] que habilita várias formas de fraude, é praticada com a interceptação de dados pessoais de alguém em quantidade suficiente para o atacante poder se fazer passar pela tal pessoa. Nós colocamos demasiada informação sobre nós mesmos na rede, o que simplifica planos de ataques desse tipo. O furto de identidade não é, em sua natureza, digital *per se*, mas a rede facilita-o enormemente.

Como explica o artigo no site do Departamento da Justiça dos EUA:

[...]seus dados pessoais, particularmente o número de Seguro Social, sua conta bancária, número de cartão de crédito, número de cartão telefônico e outros dados importantes de identificação podem ser utilizados, quando ficarem nas mãos erradas, para obter ganhos a seu custo[129]. [tradução do autor].

A instituição Identity Theft Resource Center tem uma classificação mais detalhada:

- roubo de identidade criminal (o ofensor ao ficar detido tenta passar por uma outra pessoa);
- roubo de identidade financeiro (utilização da identidade de um outr pessoa para obter crédito, compras bens ou serviços);
- clonagem de identidade (utilização informações sobre uma outra pessoa para passar por ela na vida cotidiana);
- roubo de identidade médico (utilização de identidade alheia para obter serviços)
- roubo de identidade de crianças (utilização de identidade de uma criança)[130].

Devemos observar que os dados pessoais podem, mas não precisam ser obtidos através da rede aberta. No caso da rede, o roubo de identidade pode começar, por exemplo, por meio de phising, ou em resultado de invasão de com intuito de “roubar” (vazar) nomes de login e senhas para sites que contém dados pessoais, ou por meio de contaminação por malware (cavalo de Troia) ou spyware. Fora da rede, o roubo de identidade pode acontecer em resultado de perda, furto ou roubo de carteira, vazamento de dados oficiais, como por exemplo registros médicos. Os ofensores podem, também, obter os nossos dados pessoais vasculhando as lixeiras em busca de documentos que levam o nosso nome, endereço e outros dados que permitem identificar-nos, ou interceptar a correspondência endereçada para nós (por exemplo, em ofertas para aquirir um cartão de crédito).

O artigo do Departamento da Justiça citado acima convoca o caso real de roubo de identidade em que o ofensor causou a um casal danos financeiros de mais que 100 mil dólares, recebeu crédito federal imobiliário, comprou casas, motocicletas e armas em nome das vítimas. A restituição de suas identidades custou as vítimas ainda 15 mil de dólares e levou quatro anos de tormento em suas vidas.

As estatísticas referentes aos casos de roubo de identidade são alarmantes. O Birô de Estatísticas da Justiça dos EUA publicou um relatório[131] no qual 8,6 milhões de agregados familiares tiveram pelo menos uma pessoa de 12 anos ou mais que foi vítima de roubo de identidade em 2010. Em 2005, este número foi de 6,4 milhões, mostrando um aumento de 34% em apenas 5 anos. Na dimensão financeira, os danos causados por este crime em 2010

128 Artigo 299 do Código Penal Brasileiro de 1940.

129 The United States Departent of Justice, http://www.justice.gov/criminal/fraud/websites/idtheft.html (carregado em 23 de junho de 2013).

130 Identity Theft Resource Center, http://www.idtheftcenter.org/ (carregado em 23 de junho de 2013).

131 Bureau of Justice Statistics, "Identity Theft Reported by Households, 2005-2010", http://www.bjs.gov/index.cfm?ty=pbdetail&iid=2207 (carregado em 23 de junho de 2013).

totalizaram 13,3 bilhões de dólares, sendo em mídia 2200 dólares por agregado (contando apenas os que perderam pelo menos um dólar).

Em 2012, a empresa id:analytics conduziu uma pesquisa que demonstrou algo bastante surpreendente: nos EUA, aproximadamente 2,5 milhões roubos de identidade cada ano estão relacionados com cidadãos Americanos falecidos.[132]

O roubo de identidade vai muito além da invasão da privacidade. Ele invade brutalmente toda a vida da vítima e da sua família e é um acontecimento verdadeiramente dramático. A vítima tem de provar que não cometeu fraudes ou crimes que foram cometidos usando sua identidade. Isso nunca é fácil, às vezes até impossível, e a vítima é de fato tratada como criminoso, o que é uma experiência psiquicamente devastadora. A restituição de reputação, além de ser difícil, lenta e cara, pode, também, não ser plena ou mesmo possível e pode estigmatizar a vítima para o resto da sua vida,estendendo efeitos devastadores na vida de sua família.

4. Defesa da privacidade na rede aberta

4.1. Introdução

A defesa da privacidade na rede aberta é uma questão não menos complexa que a definição mesma de privacidade, e do que os motivos e métodos da sua erosão, metodicamente planejada ou ocorrida via efeito colateral. Alem disso, todos estes aspetos influenciam-se dinamicamente e se transpassam a si mesmos.

Craig e Ludloff caraterizam a questão de privacidade no mundo contemporâneo como uma "tempestade perfeita". Isso sugere um estado de confrontação descontrolada e imprevisível de grandes forças e, de fato, a nós também nos parece que deve ser assim percebido. Conforme estes autores, não existem métodos para defender a privacidade que possam ser identificados como definitivos, sem que isso signifique que ela não deva ser protegida[133].

Vamos tentar definir quem tende a proteger a privacidade de usuários na rede aberta, e como. Infelizmente, já esta categorização, aparentemente simples, resulta em uma multidão de possíveis acepções. A questão da defesa da privacidade na rede na época digital tem, pelo menos, quatro dimensões principais:

- legal;
- tecnológica (informática);
- social;
- comportamental.

A defesa legal significa que para proteger a privacidade adotam-se várias normas e leis em vários níveis normativos (global, transnacional, regional, nacional, local, etc.).

Por defesa tecnológica denominamos o conjunto de ações de caráter informático que visam erradicar ou pelo menos limitar as ameaças à privacidade. Isso, essencialmente, significa criar softwares e/ou manipular os parâmetros da comunicação pela rede, criptografar dados, anonimizar comunicações, etc. para combater as ações ou intenções de vários invasores ou atores que operam como “cupins” da privacidade alheia.

A defesa social manifesta-se pelas atividades de organizações e movimentos sociais a favor da proteção da privacidade (buscar e informar-se e ao público sobre as ameaças, educar, fazer petições públicas, organizar manifestações, etc.).

---

132 id:analytics. "Identities of Nearly 2.5 Million Deceased Americans Misused Each Year", http://www.idanalytics.com/news-and-events/news-releases/2012/4-23-2012.php (carregado em 23 de junho de 2013).

133 Terence Craig e Mary E. Ludloff, "Privacy and Big Data", p. 1.

Finalmente, a defesa comportamental é ligada às nossas ações como pessoas físicas cuja privacidade é potencialmente ou realmente invadida ou subvertida (ela pode e deve ser acrescentada à dimensão social).

Aparentemente, enfrentamos problemas sérios em todas estas dimensões. Na área do direito, observamos o atraso ou falta da legislação adequada, falta ou fraqueza de ações executivas e, em casos de alguns países, também falta de vontade efetiva de proteger a privacidade dos usuários da rede (e cidadãos com tais) por motivos políticos e/ou comerciais. Temos também o problema, já fortemente sinalizado, da falta de percepção geral do que é a privacidade, e que ela resulta de um mosaico de leis e costumes no mundo todo, em vários níveis, frequentemente não compatíveis entre si. É importante frisar que a complexidade da tecnologia moderna causa uma falta crônica de entendimento coerente e de peritos da área.

A defesa tecnológica é frequentemente submetida a alguma "solução" comercial, justamente na esfera que é constitui um dos fatores invasores,onde então enfrentamos contradições e conflitos de interesses. Esta defesa é, via de regra, demasiadamente complicada para os usuários comuns.

Os movimentos sociais enfrentam problemas na sua atividade, pois os usuários não os escutam, ou não sabem da sua existência, ou não lhes dão importância, que por isso encontram dificuldades de levantar recursos, e se não há pressão destes movimentos sobre os órgãos administrativos, estes não se sentem obrigados ou forçados a agir em defesa da privacidade dos cidadãos.

No caso da dimensão comportamental, observamos uma inércia ingênua dos usuários na sua interação com a rede, adoção de padrões (moda) que são efetivamente contraditórios à proteção da privacidade, negligência ou incompreensão de riscos, conduta subliminarmente estimulada pela indústria que mercadeja dados pessoalizáveis.

4.2. Defesa legal

4.2.1. Fundamentos legais

A presente monografia limita-se aos aspetos da interação de usuários com a rede aberta e não pretende oferecer uma análise da questão jurídica envolvida na conceituação ou na definição de privacidade, suas ameaças e medidas de defesa. Em verdade os problemas com a privacidade na sua "manifestação digital", que resumidamente chamamos de "privacidade digital", são apenas uma parte, embora não a menos significativa, dos problemas com a privacidade no sentido global, que fazem parte dos problemas da condição humana com tal, na era digital. Nos limitamos à convocação dos fundamentos legais, das tendências atuais na legislação nos países mais relevantes neste sentido, fazendo observações sobre a "privacidade digital" que deve fazer parte da privacidade geral ou "tradicional", mas que aparentemente nem sempre o faz.

A defesa da privacidade tradicional já se embutiu em vários níves da legislação de praticamente todos os países do mundo, seja em suas Constituições ou em leis de regimes consuetudinários (cabe ressaltar que, por exemplo, o Reino Unido não possui na sua legislação um ordenamento constitucional). Os EUA não têm na sua Constituição nenhuma invocação à defesa da privacidade, mas os emendas e várias leis ordinárias tratam deste assunto.

Existem quadros internacionais que serviram de base para criação de leis sobre proteção à privacidade em níveis infraconstitucionais, como leis regionais e nacionais ordinárias. O mais fundamental deles é a Declaração Universal dos Direitos Humanos da ONU, de 1948. No seu artigo 12 as Nações Unidas proclamam:

Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques a sua honra e reputação. Todo o homem tem direito à proteção da lei contra tais interferências ou ataques[134].
Este documento é formalmente de aceitação obrigatória para todos os membros da ONU.

Em 1950, foi adotada, pelo Conselho da Europa, a Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais[135], que entrou em vigor em 1953. Cabe ressaltar que o Conselho da Europa não é um órgão administrativo, embora tenha personalidade jurídica amplamente reconhecida. Três países da região: Cazaquistão, Bielorrússia e Vaticano, não são membros deste organismo (até 2013). O artigo 8 desta Convenção proclama:

Direito ao respeito pela vida privada e familiar

1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.

2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) definiu em 1980 oito princípios básicos da privacidade digital que referem-se a: limitação de coleta de dados, sua qualidade, especificação de objetivo da coleta, limitação de uso, segurança, abertura, participação individual e responsabilidade[136]. Este documento ainda serve como uma base para construção normativa em legislações nacionais[137]. Os instrumentos legais da UE têm muitas ligações com os postulados da OCDE.

O problema atualmente candente é que a "privacidade digital" parece já não caber nestas definições dos anos 40, 50, 80 e até nos mais recentes. O desenvolvimento da tecnologia se acelera e os riscos referentes a privacidade e liberdade multiplicam-se. Assim, vários países e seus agrupamentos têm que introduzir ou redefinir as leis sobre a proteção da privacidade para confrontarem o presente e o futuro.

A interação de usuários com a rede aberta cai na área vasta de legislação chamada "proteção de dados pessoais". A primeira lei sobre proteção de dados pessoais no mundo surgiu no estado de Hesse na Alemanha, em 1970. A ideia desta lei foi de defender os acervos estatais de dados pessoais sobre cidadãos contra abusos por parte de funcionários. Foi esta lei que, pela primeira vez, mencionou a criação de uma instituição independente denominada "oficial de proteção"[138]. Em nível nacional, o primeiro ato legislativo foi o da Suécia (1973), depois dos EUA (1974), da Alemanha (1977) e da França (1978). Em 2005, aproximadamente 50 países do mundo adotaram leis sobre a proteção de dados pessoais[139]. Em 2013, o Information Shield publicou um índice dos mais que 60 países que adotaram tais leis[140].

Um dos problemas atuais na área da proteção da privacidade por meios legais é a

134 Declaração Universal Dos Direitos Humanos Adotada e proclamada pela resolução 217 A (III) da Assembléia Geral das Nações Unidas em 10 de dezembro de 1948. O texto completo pode ser encontrado em muitos lugares, por exemplo, na página oficial do Ministério da Justiça do Brasil: http://portal.mj.gov.br/sedh/ct/legis_intern/ddh_bib_inter_universal.htm (carregado em 25 de maio de 2013).

135 http://www.echr.coe.int/Documents/Convention_POR.pdf

136 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part2 (carregado em 3 de julho de 2013).

137 Em 2013, OCDE tem 34 países membros.

138 J.B. Rule, G Greenleaf, "Global Privacy Protection, The First generation", p. 92.

139 Ibid.

140 http://www.informationshield.com/intprivacylaws.html (carregado em 3 de julho de 2013).

incompatibilidade dos sistemas nacionais no mundo globalizado que, a propósito, limita as possibilidades do desenvolvimento do comércio eletrônico compatível.

4.2.2. União Europeia

A questão da privacidade ocupa um lugar destacado na discussão pública, na Europa. Os povos europeus lembram-se bem dos tempos da agressão nazista e de sistemas opressivos no bloco de leste ligados à União Soviética. Esta memoria é particularmente forte na Alemanha mesma. Não é difícil prever o que teria acontecido se o Gestapo ou, depois da Segunda Guerra, a Stasi na Alemanha Oriental tivessem disposto da tecnologia contemporânea[141]. Esta mentalidade na Europa tem uma base forte na convicção de que o excesso de poder causado pela acumulação, clandestina ou não, de informações sobre indivíduos invade sua liberdade e privacidade e pode levar a confrontos sangrentos.

O alvo da política da UE para proteção de dados pessoais é manter o equilíbrio entre o nível alto da proteção da vida privada e a transferência livre dos dados pessoais dentro da UE. Por isso, existe um limite estrito de coleta e uso de dados pessoais e todos os países do bloco são obrigados a estabelecer um órgão nacional independente que seja responsável pela proteção destes dados. O ato mais fundamental na UE hoje é a Diretiva 95/46/CE[142] cujos princípios são[143]:

- *A **qualidade** dos dados: os dados pessoais devem, designadamente, ser objecto de um tratamento leal e lícito, e ser recolhidos para finalidades determinadas, explícitas e legítimas. Devem, além disso, ser exatos e, se necessário, atualizados.*
- *A **legitimidade** dos tratamentos de dados: o tratamento de dados pessoais só poderá ser efetuado se a pessoa em causa tiver dado de forma inequívoca o seu consentimento ou se o tratamento for necessário para:*
- *a execução de um contrato no qual a pessoa em causa seja parte ou*
- *o cumprimento de uma obrigação legal à qual o responsável pelo tratamento esteja sujeito ou*
- *a proteção de interesses vitais da pessoa em causa ou*
- *a execução de uma missão de interesse público ou*
- *a prossecução de interesses legítimos do responsável pelo tratamento.*
- *As **categorias** específicas de tratamentos: deve proibir-se o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual. Esta disposição comporta reservas relativas, por exemplo, a casos em que o tratamento seja necessário para proteger interesses vitais da pessoa em causa ou para efeitos de medicina preventiva e diagnósticos médicos.*
- *A **informação** das pessoas objecto dos tratamentos de dados: o responsável pelo tratamento deve fornecer à pessoa em causa junto da qual recolha dados que lhe digam respeito um certo número de informações (identidade do responsável pelo tratamento, finalidades do tratamento, destinatários dos dados, etc.).*
- *O **direito de acesso** destas pessoas aos dados: todas as pessoas em causa devem ter*

141 Após a revelação de segredos da Stasi, o mundo ficou chocado com o nível tecnologico, psicologico e alcance da espionagem efetuada pela Stasi. Ver por exemplo: Kristie Macrakis, "Seduced by Secrets: Inside the Stasi's Spy-Tech World".

142 Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, Jornal Oficial nº L 281 de 23/11/1995 p. 0031 – 0050, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:PT:HTML (cerregado em 3 de julho de 2013).

143 Europa, Sínteses da legislação da UE. http://europa.eu/legislation_summaries/information_society/data_protection/l14012_pt.htm.

o direito de obter do responsável pelo tratamento:

- *a confirmação de terem ou não sido tratados dados que lhes digam respeito e a comunicação dos dados sujeitos a tratamento;*
- *a retificação, o apagamento ou o bloqueio dos dados cujo tratamento não cumpra o disposto na presente diretiva, nomeadamente devido ao carácter incompleto ou inexato dos dados - bem como a notificação dessas alterações aos terceiros a quem os dados tenham sido comunicados.*
- *As **derrogações e restrições**: o alcance dos princípios relativos à qualidade dos dados, à informação da pessoa em causa, ao direito de acesso e à publicidade dos tratamentos pode ser restringido a fim de salvaguardar, por exemplo, a segurança do Estado, a defesa, a segurança pública, a repressão de infracções penais, um interesse econômico ou financeiro importante de um Estado-Membro ou da UE, ou a proteção da pessoa em causa.*
- *O **direito de oposição** aos tratamentos de dados: a pessoa em causa deve ter o direito de se opor, por motivos legítimos, a que os dados que lhe digam respeito sejam objecto de tratamento. Deve igualmente poder opor-se, a seu pedido e gratuitamente, ao tratamento de dados previsto para efeitos de prospecção. Deve ainda ser informada antes de os dados serem comunicados a terceiros para efeitos de prospecção e ter o direito de se opor a essa comunicação.*
- *A **confidencialidade e segurança do tratamento**: qualquer pessoa que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante (bem como o próprio subcontratante), tenha acesso a dados pessoais, não pode tratá-los sem instruções do responsável pelo tratamento. Por outro lado, o responsável pelo tratamento deve pôr em prática medidas adequadas para proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizado.*
- *A **notificação** dos tratamentos a uma autoridade de controlo: o responsável pelo tratamento deve notificar a autoridade de controlo nacional antes da realização de qualquer tratamento. Após a recepção da notificação, a autoridade de controlo procede a exames prévios sobre eventuais riscos relacionados com os direitos e liberdades das pessoas em causa. Deve assegurar-se a publicidade dos tratamentos e as autoridades de controlo deverão manter um registo dos tratamentos notificados.*

Adicionalmente:

*Qualquer pessoa deve poder **recorrer aos tribunais** em caso de violação dos direitos que lhe são garantidos pelas disposições nacionais aplicáveis ao tratamento em questão. Além disso, qualquer pessoa que tiver sofrido um prejuízo devido a um tratamento ilícito de dados pessoais que lhe digam respeito tem o direito de obter reparação pelo prejuízo sofrido*[144].

Por causa de vários fatores ocorrendo no mundo globalizado, como por exemplo a transferência de dados em escala global, computação em nuvem, etc. a diretiva em questão está sendo renovada graças a proposta da Comissão Europeia de 25 de janeiro de 2012. Em 2013, o Parlamento Europeu debate sobre as seguintes questões[145]:

- "**Direito a ser esquecido**" – graças às novas regras legais, usuários obterão a possibilidade de solicitar a remoção de seus dados pessoais. O problema é de definir

144 Ibid.

145 Parlamento Européu, Birô de Informações na Polônia, http://www.europarl.pl/pl/Aktualnosci_i_zaproszenia/Aktualnosci/news/news-2013/news_2013_June/ulotka_ochrona_prywatnosci_2013.html;jsessionid=269EA3CA15B934EEDC749636BE82444A. (cerregado em 6 de julho de 2013).

os limites de tal opção e suas consequências no que, por exemplo, diz respeito à liberdade de se pronunciar[146];

- **Perfilamento de usuários** – várias entidades colecionam os dados pessoais para analisar e prever as atitudes e comportamento de usuários (compras, interesses, emprego, estado de saúde, etc.). Regularizar este fenômeno não parece ser uma tarefa fácil;
- **Consentimento expresso** de usuário para uso de seus dados – as entidades que processam estes dados terão de obter a permissão clara do usuário. Isso gera vários problemas técnicos e legais na organização de sistema de gerenciamento destas permissões;
- **Acesso aos dados e sua transferência** – a nova lei vai permitir aos usuários a acessar seus dados e transferi-los para um outro provedor de serviço. É necessário definir os limites dessas possibilidades;
- **Penalização de abusos** – para proteger os dados pessoais devemos introduzir penas. A questão é de quão severas elas devem ser.

A UE tende a estabelecer um único ato normativo denominado *General Data Protection Regulation* (GDPR). A adoção deste ato é prevista para 2014, com um período de de transição de dois anos (deve entrar em vigor em 2016)[147].

O papel da legislação da UE é importante na escala global. Estas leis servem como padrão, ponto de referência ou incentivo para outros países e blocos. Por exemplo, o Canada adotou o seu ato PIPEDA (Personal Information Protection and Electronic Documents Act) em 2000, mesmo para manter a compatibilidade com a legislação da UE, o que visava o desenvolvimento do comércio eletrônico[148]. Um dos fundamentos da legislação europeia é que não é permitido transferir os dados pessoais a países terceiros que não garantam os mesmos níveis de proteção a estes dados.

A circulação livre de dados pessoais é permitida só no Espaço Econômico Europeu (que além dos países da UE inclui: Islândia, Liechtenstein e Noruega). Para resolver este assunto surgiram os processos (pactos) de cooperação entre os EUA e a UE (U.S. – European Union Safe Harbor Framework[149]) e, também, entre EUA e a Suíça (U.S.-Switzerland Safe Harbor Framework[150]). Estes processos prevêem a possibilidade de transferência de dados entre as entidades sediadas na UE e as de fora da UE no caso de estas adotarem voluntariamente os princípios da Diretiva 95/46/CE da UE. O fato de adotar estes princípios é difícil de fiscalizar e existem, pelos menos, três documentos altamente críticos em relação ao pacto Safe Harbor entre a UE e os EUA:

- *The application of Commission Decision on the adequate protection of personal data provided by the Safe Harbor Privacy Principles* (2002)[151];
- *The implementation of Commission Decision on the adequate protection of*

146 Por enquanto, este direito foi, pelo menos parcialmente, vetado pelo Tribunal da EU (em 25 de junho de 2013). Um conselheiro do Tribunal da Justiça da EU afirma que o Google não tem de remover as informções pessoais no resultados de busca, mesmo que estas informações sejam destrutivas para a preputação de um indivíduo. J. Vincent, Independent, "EU court rules in Google's favour: 'right to be forgotten' vetoed", http://www.independent.co.uk/news/world/europe/eu-court-rules-in-googles-favour-right-to-be-forgotten-vetoed-8672512.html (carregado em 3 de julho de 2013).

147 Wikipédia, artigo "General Data Protection Regulation", http://en.wikipedia.org/wiki/General_Data_Protection_Regulation (carregado em 3 de julho de 2013).

148 Wikipédia inglesa, artigo " Personal Information Protection and Electronic Documents Act", http://en.wikipedia.org/wiki/Personal_Information_Protection_and_Electronic_Documents_Act (carregado em 3 de julho de 2013).

149 http://export.gov/safeharbor/

150 Ibid.

151 http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/sec-2002-196/sec-2002-196_en.pdf (carregado em 3 de julho de 2013).

personal data provided by the Safe Harbor Privacy Principles (2004)[152];

- *US Safe Harbor - Fact or Fiction?* (2008)[153].

Estes relatórios demonstram numerosas falhas por parte das entidades americanas: declarações de participação falsas, declarações de certificação falsas, abusos na utilização da marca de certificação, afirmações incompletas ou enganosas sobre as políticas de privacidade e muitos outros problemas.[154]

4.2.2. Estados Unidos

Embora a Constituição dos EUA não mencione diretamente o termo privacidade, neste pais existem dezenas de leis que regulamentam esta questão, inclusive na sua "dimensão digital", tanto no nível federal, como em legislações estaduais[155]. Este fato gera, efetivamente, um caos, especialmente, quando os EUA precisam colaborar com o exterior, na questão da proteção de dados pessoais.

O problema é muito grave, pois a Internet nasceu naquele país e, em resultado, lá surgiram os novos modelos de negócios que, em sendo promissores, acabam por destruir a privacidade de usuários na rede, em todo o mundo. Os EUA não se gerenciam pelas mesmas preocupações de natureza humana que fundamentam as legislações dos países da UE. Nos EUA nunca surgiram regimes realmente totalitários e opressivos, embora as guerras contra narcóticos, pornografia e terrorismo, programas como Echelon, PRIS, etc. sinalizem que este país está rumando para um novo tipo de "totalitarismo", composto por vigilância global sem controle e pelo padrão obrigatório do consumerismo que Aldous Huxley, já em 1932 (depois em 1958 e em 1962), apresentou como uma escravidão contemporânea, comparada com a religião[156].

No mundo norte-americano, as novas tecnologias são percebidas como novas vantagens comerciais. O dinheiro é a única medida de sucesso e da condição humana. Nenhuma outra media parece ser viável, como demostram os modelos de negócio das mais destacadas empresas norte-americanas, como o Facebook e o Google.

Os atos normativos mais relevantes na legislação dos EUA são *The Privacy Act*, de 1974, e *The Computer Matching and Privacy Act*, de 1988. Estas leis tratam exclusivamente dos dados pessoais guardados pelo Governo Federal, e que não exercem nenhum poder sobre a coleta e uso de dados e informações pessoais por outros sujeitos, privados ou públicos[157].

Nos últimos anos, nenhum país do mundo seguiu os exemplos legislativos dos EUA[158]. Vários países do mundo adotaram recentemente as leis sobre a proteção de dados pessoais conforme os padrões europeus, entre eles a Argentina[159].

---

152 http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/sec-2004-1323_en.pdf (carregado em 3 de julho de 2013).

153 Chris Connolly (Galexia), Privacy Laws and Business International, issue 96, December 2008; http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf (carregado em 3 de julho de 2013).

154 Ibid.

155 Information Shield, http://www.informationshield.com/usprivacylaws.html (carregado em 3 de julho de 2013).

156 Wikipédia inglesa, artigo "Brave New World", http://en.wikipedia.org/wiki/Brave_New_World (carregado em 3 de julho de 2013), "Brave New World Revisited" de 1958, (http://www.huxley.net/bnw-revisited/) (carregado em 3 de julho de 2013); Wikipédia inglesa, artigo "Island (novel)" de 1962, http://en.wikipedia.org/wiki/Island_%28novel%29 (carregado em 3 de julho de 2013)

157 Jean Slemmons Stratford, Juri Stratford, "Data Protection and Privacy in the United States and Europe", www.iassistdata.org/downloads/iqvol223stratford.pdf (carregado em 3 de julho de 2013).

158 Peter Fleischer: Privacy...?, "We Need a Better, Simpler Narrative of US Privacy Laws", de 12 de março de 2013, http://peterfleischer.blogspot.com/2013/03/we-need-better-simpler-narrative-of-us.html (carregado em 3 de julho de 2013).

159 International Data Protection and Privacy Law - White & Case, http://www.whitecase.com/files/Publication/367982f8-6dc9-478e-ab2f-

4.2.3. China

Durante décadas, a China foi apontada como exemplo particular na área da proteção de privacidade digital, pela razão simples de não providenciar nenhuma proteção e censurar profundamente a internet doméstica. Mas em fevereiro de 2013 apareceu um conjunto de diretrizes intituladas "*Guidelines for Personal Information Protection in Information Security Technology Public and Commercial Service Systems*" (As Diretrizes).[160]. As Diretrizes não são obrigatórias, mas, pelo menos, definem o termo "informação pessoal" e os oito princípios de coleta, processamento, transferência e remoção desta informação.

O termo "informação pessoal" faltou na legislação chinesa. As Diretrizes o definem como: *dados de computador que podem ser processados por sistema de informação, relevantes para certa pessoa natural e que podem ser utilizados sozinhos, ou junto com outras informações, para identificar tal pessoa natural.*[161] [tradução do autor].

Conforme As Diretrizes, a informação pessoal pode ser coletada somente se o usuário for previamente informado sobre: motivo e meios de coleta, informação a ser coletada, período de retenção, escopo de uso (inclusive a revelação e transferência para outras organizações e instituições), medidas de proteção, nome, endereço e contato dos sujeitos efetuando a coleta, riscos de providenciar as informações, consequências de recusar de fornecer os dados, meios de efetuar queixas. Além disso, quando a informação vai ser transferida ou entregue a uma outra organização, o usuário deve ser informado sobre: o motivo de tal transferência ou entrega, que informação, em qual escopo e para qual uso a informação vai ser transferida ou entregue, nome, endereço e dados de contatos do recebedor desta informação[162].

As Diretrizes mandam a remoção da informação pessoal quando o motivo para sua coleta for realizado[163]. A transferência não autorizada de dados da China para o exterior é proibida. Para tal transferência deve-se obter a permissão da pessoa e das autoridades competentes[164].

É claro que a China não vai parar de perseguir os oponentes políticos e censurar a rede, mas As Diretrizes constituem um passo adiante significativo, pelo menos para ser aplicada aos concorrentes privados do vigilantismo local. A China teria que respeitar as regras básicas, inclusive as internacionais, que são essenciais para sua expansão econômica[165].

4.2.4 Rússia

A Rússia adotou uma lei intitulada "A Lei Federal sobre Os Dados Pessoais", em 2006 (com alterações seguintes em 2009, 2010 e 2011)[166]. A lei define o termo "Operador de Dados Pessoais" que é: *órgão estatal, órgão municipal, pessoa jurídica ou física que organiza e/ou*

5fdf2d96f84a/Presentation/PublicationAttachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_IntlDataProtectionandPrivacyLaw_v5.pdf (carregado em 3 de julho de 2013).

160 InsidePrivacy, "China Releases National Standard for Personal Information Collected Over Information Systems; Industry Self-Regulatory Organization Established", de 25 de janeiro de 2013, http://www.insideprivacy.com/international/china-releases-national-standard-for-personal-information-collected-over-information-systems-industr/ (carregado em 3 de julho de 2013).

161 Ibid.

162 Ibid.

163 Ibid.

164 Ibid.

165 The Economist, "The long march to privacy", http://www.economist.com/node/5389362 (carregado em 6 de julho de 2013); Making Sense of China's New Privacy Laws, The Hogan Lovells Privacy Team, de 28 de junho de 2013, https://www.privacyassociation.org/privacy_tracker/post/making_sense_of_chinas_new_privacy_laws (carregado em 6 de julho de 2013).

166 Wikipédia russa, artigo: "Федеральный закон «О персональных данных»", http://ru.wikipedia.org/wiki/Федеральный_закон_«О_персональных_данных» (carregado em 6 de julho de 2013).

efetua o processamento de dados pessoais, bem como determina os alvos e conteúdos do processamento de dados pessoais.[167].

Conforma a Lei, os dados pessoais são qualquer informação sobre o "sujeito de dados pessoais" identificado ou identificável por tal informação. A Lei enumera as categorias desta informação: nome, sobrenome, patronímico, data e lugar de nascimento, endereço, família, status social, status de propriedade, educação, profissão, remuneração, etc. Além disso, a Lei determina os dados pessoais sensíveis, como: raça, etnia, opiniões políticas, religião e crença, saúde e vida sexual[168].

A Lei concede certos direitos aos sujeitos de dados pessoais. Eles têm direito de:

- acessar os dados acumulados pelo operador bem como os dados sobre o operador mesmo;
- demandar encerramento do processamento, bloqueio ou modificação de dados pessoais que foram obtidos ilicitamente, são inadequados ou desatualizados;
- demandar o encerramento imediato de processamento de dados com motivos do marketing direto.[169] (Isso é muito interessante).

A Lei russa é frequentemente criticada pelos peritos por causa da sua generalidade. Ela ainda tem que ser revistada e modificada[170].

4.2.5. Brasil

Em 2013, o projeto da lei brasileira sobre proteção de dados pessoais ainda é discutido[171]. O Brasil permanece o único país no Mercosul que ainda não possui tal legislação. Cabe ressaltar que, mesmo não possuindo tal legislação, o Brasil utiliza a votação eletrônica nas eleições.

O Brasil é um dos alvos principais dos ataques de hackers no mundo[172].

O Governo e a Justiça brasileiros são uns dos maiores requerentes dos dados pessoais do Google[173] (8% de requisições mundias ao Google, em 2012).

No Brasil existe o comércio ilícito de dados pessoais que vazaram dos bancos de dados teoricamente sigilosos das várias instituições públicas (Receita Federal, INSS, Detran) e privadas, como seguradoras de veículos. Os dados são comercializados na Internet e até nas ruas[174].

Sem dúvida, o Brasil deve adotar uma lei sobre proteção de dados o quanto antes, tanto para regularizar a situação interna, como para impulsionar o desenvolvimento do comércio eletrônico compatível com a globalidade.

---

167 Wikipédia russa, artigo: "Оператор персональных данных", http://ru.wikipedia.org/wiki/Оператор_персональных_данных (carregado em 6 de julho de 2013).

168 Wikipédia inglesa, artigo: " Data protection (privacy) laws in Russia ", http://en.wikipedia.org/wiki/Data_protection_%28privacy%29_laws_in_Russia (carregado em 6 de julho de 2013).

169 Ibid.

170 Алексей Королюк (Aleksey Koroliuk), CNews, Эксперты: закон «О персональных данных» нужно доработать, de 30 de junho de 2011, http://internet.cnews.ru/news/line/index.shtml?2011/06/30/445794 (carregado em 6 de julho de 2013).

171 Vale pena consultar a história desta discussão na Wikipédia portuguesa, artigo "Marco Civil da Internet", http://pt.wikipedia.org/wiki/Marco_Civil_da_Internet (carregado em 6 de julho de 2013).

172 M. Campi, Info Online, "Brasil é o 4ª principal alvo de roubo de dados online", de 10 de junho de 2013, http://info.abril.com.br/noticias/seguranca/brasil-e-o-4-principal-alvo-de-roubo-de-dados-online-10062013-21.shl (carregado em 6 de julho de 2013).

173 J. Chade, ESTADÃO.COM.BR/Internacional, "Brasil é o 3º país que mais pede dados ao Google", http://www.estadao.com.br/noticias/impresso,brasil-e-o-3-pais-que-mais-pede-dados-ao-google-,1040131,0.htm (carregado em 6 de julho de 2013).

174 B. Tavares, C. Stanisci, R. Burgarelli e B. Boghossian, ESTADÃO.COM.BR, "Informação pessoal vale R$ 100", de 19 de agosto de 2010, http://blogs.estadao.com.br/jt-seguranca/tag/comercio/page/2/ (carregado em 6 de julho de 2013).

4.3. Defesa com uso de ferramentas informáticas

4.3.1. Anonimização e criptografia (Projeto Tor)

Como já foi mencionado, o endereço IP do cliente pode revelar surpreendentemente muita informação. A proteção do IP do computador do usuário tem por motivo esconder do servidor este endereço durante a requisição e a resposta. Existem métodos relativamente simples de atingir esse alvo.

Na cadeia de roteadores que ficam entre o computador-cliente e o computador-servidor deve-se introduzir mais um computador (roteador), chamado de servidor *proxy,* com a função especial de trocar o endereço do cliente pelo seu próprio endereço IP. Desse jeito, o servidor final não pode determinar de onde vem a requisição original ou se ela mesmo aconteceu. Do ponto de vista dele, destinatário, a requisição vem do servidor *proxy*. Na prática, a comunicação pode passar por mais de um computador com a função de *proxy* (multiplicidade de *proxies*). Isso diminui significativamente a probabilidade de se poder descobrir a fonte da requisição. A condição necessária para manter o sigilo do IP original é de não preservar nenhuma informação sobre a origem e o destino da requisição em *logs,* ou de outra maneira, em servidores *proxy*. Esse tipo de proteção recebeu o nome de anonimização.

Infelizmente, a realidade não corresponde com o nosso objetivo de ficar anônimos. Antes de mais nada, já na primeira etapa da comunicação http – do computador do usuário ao servidor do provedor da Internet – já se revela quem inicia a comunicação destinada a quem, ainda antes de essa comunicação atingir o computador designado como o nosso primeiro *proxy* (falamos aqui sobre um roteiro comum envolvendo um usuário de banda larga). As empresas provedoras de acesso a Internet têm que subordinar-se às leis, que frequentemente as obrigam a manter os *logs* de comunicação passando pelos seus servidores, pelo menos durante um tempo predeterminado. As empresas que prestam os serviços comerciais de anonimização podem ser limitadas pelas mesmas leis. O máximo que um usuário pode conseguir é esconder o seu IP do servidor final. Mas mesmo assim, as ferramentas programáticas modernas permitem inferir sobre a origem da requisição utilizando as técnicas de agregação de dados e de casamento de padrões. Além disso, utilizando os serviços de anonimização deve-se lembrar que nunca se pode estar certo de que a empresa contratada verdadeiramente faz o que oferece. Agrupando as requisições de milhares de usuários, as empresas provedoras de acesso a Internet e as empresas prestando os serviços de anonimização obtém as informações sobre nós e sobre o fluxo de informação, e isto tem grande valor comercial. Logo, a questão da nossa confiança nestes serviços é fundamental.

Na era digital, criptografar corretamente informações e comunicações é indispensável. No caso da interação com a rede aberta, os métodos criptográficos utilizam-se na navegação pela www (https), na correspondência de e-mail e também no nível menor de comunicação, por exemplo em ligações WiFi ou em comunicações TCP/IP (Transport Layer Security - TLS). Hoje, a PGP (Pretty Good Privacy) é uma ferramenta popular que permite criptografar e decifrar os e-mails, arquivos e assiná-los digitalmente e verificar a identidade do remetente[175].

Existem projetos abertos que utilizam os computadores de usuários como servidores de *proxy* junto com a criptografia. Examinaremos um exemplo chamado Tor.

Projeto Tor[176]

O projeto Tor (The Onion Router – Roteador Cebola), inicialmente apoiado pela Marinha dos EUA, baseia-se na ideia de se criar uma rede de computadores de usuários na qual uma requisição de página web ou de outro recurso passa pelas máquinas de vários

175 Wikipédia inglesa, artigo "Pretty Good Privacy", https://en.wikipedia.org/wiki/Pretty_Good_Privacy (carregado em 7 de julho de 2013).

176 Wikipédia inglesa, artigo "Tor (anonimity network)", https://en.wikipedia.org/wiki/Tor_%28anonymity_network%29 (carregado em 7 de julho de 2013).

usuários, escondendo assim o IP do computador que faz a requisição original. Isso é, em princípio, uma multiplicação de *proxies*, já mencionada, mas neste caso ela é dinâmica. A rota de comunicação é escolhida aleatoriamente e mantida durante o tempo da sessão e pode ser trocada automaticamente se um nó na cadeia de proxies desaparece ou quando o usuário pede gerar uma nova rota. O computador que é o último nó na cadeia faz a requisição ao servidor Http, recebe a resposta e envia de volta através dos nós, na inversa sequência, ao computador que iniciou a requisição. Com isso, tendo dois ou mais computadores-nós, é muito difícil saber de onde vem e para onde vai uma requisição. Os computadores dentro da rota só se comunicam com seus dois vizinhos. Os usuários podem requerer a geração de uma nova rota em qualquer momento. Podem também deletar os nós intermediários da cadeia, forçando assim sua redefinição automática. A rota que começa por um IP diferente do IP original do computador é chamada de "identidade".

Os computadores dentro da rede Tor podem ser tanto clientes como servidores desse serviço, i.e., podem tanto utilizar apenas o serviço de anonimização (nó de entrada), quanto podem servir como nós intermediários (*non-exit relays*) ou nós finais na sequência (*exit relays*). Eles podem também exercer todas essas funções ao mesmo tempo. Os IPs de computadores-nós na sequência são conhecidos do usuário dessa sequência, mas traçar a rota até o IP do computador que iniciou a requisição é difícil, pelo menos do ponto de vista do servidor de http que recebeu a requisição do nó final da rota.

Essa ideia é muito promissora em relação à proteção da privacidade, especialmente quando combinada com a criptografia da comunicação (https) e com a desistência de cookies e de outras tecnologias que possam revelar a identidade do usuário, como suplementos aos *navegadores*, dentre os quais o Macromedia Flash destaca-se negativamente. Essas observações já encontraram uma resposta adequada por parte dos criadores do Tor. Além do conceito dos *proxies* dinâmicos multiplicados, o pacote de software para instalar o Tor no navegador FireFox inclui: aplicação Vidalia que gerencia a rede de nós, *navegador* FireFox pré-preparado (NoScript – um suplemento que desliga os scripts e HTTPS Everywere – um suplemento que força a utilização de http com ssl). A descrição do projeto Tor informa que a utilização de outros suplementos para o FireFox pode comprometer a privacidade. Em particular, o uso do Macromedia Flash mencionado é muito perigoso, pois ele consegue transportar a informação sobre o IP verdadeiro do computador no qual ele reside e pode gravar seus próprios cookies. A Vidalia cria um *proxy* local no computador do usuário, que então pode ser utilizada com outros navegadores, embora a segurança do IP já não possa ser garantida no mesmo nível oferecido pelo FireFox pré-configurado.

Esta ideia é tão boa que já surgem reações discriminadoras por parte da Google. Se o usuário utiliza Tor com cookies desabilitados a Google parece comparar o endereço IP do computador contra a lista de IPs de nós finais do Tor conhecidos. Ele então apresenta um página de *captcha* que mesmo preenchida pelo usuário repete-se sem fim. O motivo disso é banir a interação com a Google com uso de programas que fazem grande número de requisições para extrair informações automaticamente (robôs). O Google não confirma que existe alguma discriminação deliberada contra usuários do Tor, mas a realidade é diferente. O Tor se crescer se tornaria altamente perigoso para o negócio dos motores de busca e outros colecionadores de dados pessoais em massa.

O Tor funciona, mas tem suas desvantagens. Ele é relativamente lento, pois a informação passa por muitas máquinas e é criptografada. Ele parece ser combatido pela Google, então os autores já incluíram uma detecção de *captchas* da Google e exibem uma caixa de dialogo que oferece mudar para outro motor de busca. Isso dificulta o trabalho do usuário leigo. Além disso, surge uma percepção de que os autores tendem a apoiar as pesquisadoras desejadas, então perdem a objetividade. O problema crucial da rede Tor é que ela é muito pequena, por enquanto. Para ser uma solução séria, ela precisa crescer e ganhar

mais nós intermediários e de saída. O ideal (infelizmente, completamente improvável) seria uma rede na qual participam todos os usuários da Internet. Em teoria, isso acabaria ou diminuiria significativamente a erosão da privacidade (e o negócio dos coletadores de dados), mas ao preço de carregar a rede com tráfico bem maior. Mais um problema é que o projeto Tor foi desenvolvido com a participação da marinha norte-americana, fato que pode gerar certas dúvidas em relação à inexistência de portas de fundo nos seus *softwares*, embora a organização desenvolvedora do Tor explicitamente negue a existência de *backdoors* e declara que recusará e lidará [??], se for pedida de fazer isso. As portas de fundo podem existir nos sistemas operacionais mesmos, certamente nos sistemas proprietários, então as dúvidas em relação ao Tor podem soar como exageradas. Contudo, as vantagens de se ficar suficientemente anônimo ao navegar prevalecem. Pelo menos, esconde-se a informação de utilidade comercial. O uso do Tor não é fácil de rastrear pelo servidor web no final na rota, mas isso não significa que o tráfico como tal não pode ser rastreado. Nos EUA, a legislação vigente, o Patriot Act em particular, permite a vigilância de computadores localizados neste país.

O Tor pode resolver, também, vários outros problemas, como o bloqueio da comunicação pela censura. A aplicação Vidalia permite transformar o computador do usuário aem mais um tipo de servidor chamado *bridge relay* (nó-ponta). Ele funciona da mesma maneira que os *relays* supramencionados, mas o seu endereço IP não é revelado na lista de *relays* conhecidos publicamente. Assim, os obstáculos gerados pelos provedores de serviços que bloqueiam certos números da porta ou endereços IP podem ser ignorados. Isso é de suma importância em países como a China, Rússia e outros engajados em vigilância da rede.

Reassumindo, a proteção de IP sem outros tipos de proteção do computador não é suficiente e sozinha não faz muito sentido. É preciso integrá-la com outras medidas, como a proteção contra cookies e a criptografia e sempre seguir as boas práticas descritas a seguir.

4.3.2. Proteção de e-mail

Além da criptografia corretamente utilizada, podemos e devemos proteger os nossos e-mails de várias outras maneiras.

Antes de mais nada, devemos filtrar as mensagens indesejáveis (spam). Para isso servem os filtros em programas de e-mail, mas os provedores de serviço de e-mail também podem filtrar os spam, então é bom procurar um provedor que já oferece tal opção. Na maioria dos casos os provedores de serviço de e-mail pago têm estes filtros habilitados, o que pode salvar muito tempo nosso.

É aconselhável verificar se o provedor não terceiriza os serviços de e-mail, por exemplo no serviço Gmail. É bom não utilizar os nomes verdadeiros em endereços de e-mail. Se não queremos que os nossos e-mails sejam verificados pelos robôs (indexadores automáticos), é bom não utilizar os serviços gratuitos como Gmail, Yahoo, Facebook e outros.

Além disso, ao cadastrar-se no serviço de e-mail não precisamos colocar todos os nossos dados pessoais, como nomes, sobrenome ou número de telefone. Se temos a impressão de que o provedor exige muita informação, é melhor desistir deste serviço neste servidor.

Quando carregamos um e-mail em formato HTML, os web bugs e outras técnicas podem inferir sobre os nosso interesses e verificar o fato de a mensagem ter sido aberta ou não. É aconselhável desligar os conteúdos HTML no programa de e-mail.

Uma boa ideia é possuir mais que um endereço e-mail e utilizá-los de tal maneira que a nossa identidade não seja revelada sem necessidade.

4.3.3. Proteção contra cookies, scripts, referer header e webbugs

A melhor maneira de se defender contra cookies é desabilitá-los no navegador e criar regras que os habilitam somente nos sites por nós utilizados em confiança, em particular os de caráter muito sensível, como bancos. Existem suplementos para navegadores que facilitam o

gerenciamento de cookies. Se quisermos cuidar mesmo da nossa privacidade, devemos também desinstalar o Macromedia Flash.

Os scripts também podem ser desabilitados em navegadores, mas isso, na grande maioria dos casos, vai estragar o layout de páginas e fazer a navegação praticamente impossível. Podemos, então, instalar suplementos para navegadores, como o NoScript para o FireFox, que permitem seletivamente habilitar ou desabilitar os scripts para sites específicos.

No FireFox o *referer header* pode ser alterado ou desabilitado. Existem, também, os suplementos que manipulam o parametro UserAgent o que esconde a informação sobre o nosso sistema operacional e navegador.

Os web bugs podem ser deletados do código HTML carregado ao nosso navegador por meio de suplementos que bloqueiam o web tracking, como Ghostery.

As propagandas podem ser deletadas por suplementos como AdBlock.

Existem suplementos muito originais que tendem a "diluir" o perfil do usuário na utilização dos sites de busca, como trackmenot[177]. Este programa efetua requisições aleatórias sobre as coisas irrelevantes com a frequência e a lista inicial de frases predefinidas.

Devemos sempre verificar a credibilidade dos produtores de suplementos que planejamos instalar em nossos navegadores, por exemplo buscando opiniões na rede aberta, com atenção para conteúdos suspeitos de serem mero fruto de *astroturfing* (campanha orquestrada de elogios ocultamente autopatrocinados).

4.4. Proteção de crianças

A internet é cheia de perigos e conteúdos inadequados para crianças. Devemos acompanhar a interação de crianças com a rede aberta, em particular em sites sociais que são tão populares entre jovens, hoje em dia. Existem ferramentas programáticas para auxiliar os pais, por exemplo o já citado Spector. Com certeza devemos cogitar as questões morais de monitorar as atividades de nossas crianças – é melhor falar com elas, construir um ambiente familiar de confiança, do que recorrer a espionagem.

Na rede, podemos encontrar muitos materiais dedicados a esta questão.[178]

177http://cs.nyu.edu/trackmenot/ (carregado em 6 de julho de 2013).

178 Por exemplo, no site da Microsoft, http://www.microsoft.com/pt-br/security/family-safety/childsafety-steps.aspx (carregado em 6 de julho de 2013).

Epílogo

Em vários textos sobre a privacidade, aparece com frequência o termo "Pan-óptico", cunhado por Jeremy Bentham, um utilitarista do fim do século XVIII[179]. Nesta construção linguística, o "pan" significa "geral" e "óptico" corresponde com "visível", ié, algo "oni-visível". Bentham ficou famoso por ter projetado uma cadeia em forma de uma rotunda em que as celas de prisoneiros foram colocadas circularmente em uns andares em redor de uma torre central na qual residiu um guarda-vigilante que sempre permaneceu invisível. A ideia psicológica do autor do projeto foi que a vigilância constante dos prisoneiros não era objetivamente e economicamente possível, mas a sensação de só ser possivelmente observado já podia mudar a conduta dos que estão sendo possivelmente observados, pacificando-os. Essa ideia, aparentemente muito pragmática e efetiva, é ao mesmo tempo muito desumana. O efeito em humanos, na hora de serem colocados em tal prédio ou em condições efetivamente semelhantes, ficou chamado de *"chilling effect"* ("efeito de congelamento"). O "Pan-óptico" é uma "cadeia perfeita", projetada para economizar dinheiro graças à redução do número de eventuais ações pacificadoras, na população presidiaria.

O escritor e filósofo Foucault usou esta ideia para descrever a condição da sociedade moderna, cunhando um termo "panopticismo" derivado do original "Pan-óptico"[180].

Os serviços estatais de vigilantismo à guisa de segurança de todos os países contemporâneos sempre pareceram seguir esta visão de Foucualt, mesmo antes de ela mesmo ter sido elaborada. A colocação destas instituições observadoras em um lugar não acessível, mas sensível, é bem eficaz, pois ela se baseia na intromissão a algo muito primordial – a nossa privacidade. Em geral, as modalidades mais eficazes de controle sobre humanos e seus grupos baseiam-se na exploração de caraterísticas psicológicas relacionadas aos nossos instintos e reações mais básicas, como aos riscos percebidos, (por exemplo, o “chilling effect”).

O modelo do "Pan-óptico", na sua variação comercial, continua sendo utilizado na criação, funcionamento e utilização de vários serviços oferecidos ao público. No século XXI, aparentemente concordamos com o fato de estarmos sendo observados por todos: agências do estado, empresas, empregadores, nossos próximos, colegas, etc. A ideia de observar os prisoneiros evoluiu – Foucualt, reinterpretando Bentham, traz uma obervação alarmante – somos prisoneiros de certa ideologia baseada em vigilância. Mas a vigilância de pessoas físicas (na verdade, de qualquer sujeito) não é um processo aberto ou público. Os observadores, via de regra, não publicam os efeitos desta obervação. Eles os escondem e os utilizam por motivos só por eles conhecidos.

Assim, o projeto de Bentham serve de alegoria, descrevendo a situação atual não só na rede aberta, mas também nos modelos e tendências políticas contemporâneas. O modelo atual de exercício do poder político e militar, executa-se mesmo por meio de observar e interferir sobre tudo e sobre todos; mas graças a inventos tecnológicos nunca antes presentes, estas atividades são muito mais abrangentes e possivelmente muito mais perigosas.

A privacidade da geração atual está praticamente perdida, mas não devemos nós render. Temos que lutar pela vida normal, digna e humana das nossas crianças e das gerações futuras. É preciso conscientizar as pessoas sobre a privacidade como bem fundamental, e sobre os riscos ligados à tecnologia moderna. Tentar reduzir o consumerismo e criticar os padrões narcisistas e exibicionistas de comportamento que se espalham na mídia e na vida mundana. Devemos lembrar-nos que, como consumidores, temos uma medida de defesa muito potente em nossa disposição – não comprar produtos ou serviços cuja propaganda ou cujos oferentes ofendem a nossa privacidade.

Precisamos observar os governos e suas agências calibrando nossas expectativas em relação à privacidade, liberdade e segurança nacional. Se a ameaça do terrorismo existe,

179 Wikipédia inglesa, artigo: Panpticon", http://en.wikipedia.org/wiki/Pan-óptico (carregado em 7 de julho de 2013).
180 Wikipédia inglesa, artigo: "Panopticism", http://en.wikipedia.org/wiki/Panopticism" (carregado em 7 de julho de 2013).

talvez a melhor saída seja aprender viver com medo, como isso é realidade em várias partes do globo?

Para isso tudo, precisamos da ferramenta mais potente que existe – a educação.

Referências

(na ordem do aparecimento no texto)

1. Albert J. Marcella, Jr., Carol Stucki, "Privacy Handbook, Guidelines, Exposures, Policy Implementation, and International Issues";
2. Terence Craig e Mary E. Ludolf, "Privacy and Big Data";
3. http://www.internetworldstats.com/stats.htm;
4. American Managment Association, 2007 Electronic Monitoring & Surveillance Survey, http://press.amanet.org/press-releases/177/2007-electronic-monitoring-surveillance-survey;
5. Cyberbullying Research Center, http://cyberbullying.us/;
6. The Guardian de 2 de março de 2011, artigo "You're being watched: there's one CCTV camera for every 32 people in UK" de Paul Lewis (http://www.guardian.co.uk/uk/2011/mar/02/cctv-cameras-watching-surveillance;
7. Smith David, "Orwell for Beginners";
8. Buarque de Holanda Aurélio, Novo Dicionário Aurélio da Língua Portuguesa, edição de 2004.
9. Buarque de Holanda Aurélio, Dicionário Aurélio 5ª Edição, http://www.dicionariodoaurelio.com/Privacidade.html;
10. Buarque de Holanda Aurélio, Dicionário Aurélio da Língua Portuguesa, edição de 2010.
11. Tracy Mitrano, "Civil Privacy and National Security Legislation: A Three-Dimensional View", EDUCAUSE Review, vol. 38, no. 6 (November/December 2003);
12. Wacks Raymond, "Privacy, A Very Short Introduction", Oxford University Press, 2010;
13. Arendt Hannah, "The Human Condition";
14. Warren Samuel, Brandeis Louis, "The Right to Privacy", Harvard Law Review, Vol. IV, No. 5, 15 de dezembro de 1890;
15. DeCew, Judith, "Privacy", The Stanford Encyclopedia of Philosophy (Fall 2012 Edition), Edward N. Zalta (ed.), URL = http://plato.stanford.edu/archives/fall2012/entries/privacy/;
16. Marcella Jr. Albert, Stucki Carol, "Privacy Handbook, Guidelines, Exposures, Policy Implementation, and International Issues";
17. MacKinnon Catharine A., "Reflections on Sex Equality under Law", The Yale Law Journal, Vol. 100, No. 5, Centennial Issue (Mar., 1991);
18. McKie Robin, The Observer, "Henrietta Lacks's cells were priceless, but her family can't afford a hospital", 4 de abril de 2010;
19. Harris Paul, The Observer, "Final twist to tale of Henrietta Lacks, the woman whose cells helped the fight against cancer", 31 março de 2013.
20. Hall Edward, "The Hidden Dimension", 1966
21. Wikipédia inglesa, artigo "Personal space", http://en.wikipedia.org/wiki/Personal_space
22. Senna Pires Sérgio, "Como perceber o desconforto no abraço?", http://linguagemcorporal.net.br/blog/proxemica/desconforto-no-abraco/;
23. Altman Irwin, "The environment and social behavior", Monterey, CA: Brooks/Cole (1975);
24. Wikipédia inglesa, Artigo "Catharine MacKinnon", http://en.wikipedia.org/wiki/Catharine_MacKinnon;
25. Solove Daniel J., "A Taxonomy of Privacy", University of Pennsylvania Law Review, vol. 154, no. 3, de Janeiro de 2010;
26. Westin Alan, "Privacy and Freedom", 1967;
27. Garfinkel Simson, "Database Nation, The Death of Privacy in the 21st Century";
28. Wikipédia inglesa, artigo "News International phone hacking scandal Phone-hacking scandal", http://en.wikipedia.org/wiki/News_International_phone_hacking_scandal;
29. Bamford James, "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)" no Jornal Wired, de 15 de março de 2012, http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1;
30. White House, Homeland Security dos EUA, http://www.whitehouse.gov/issues/homeland-security/ (carregado em 29 de junho de 2013).
31. White House, organograma da Homeland Security Research, http://www.homelandsecurityresearch.com/wp-content/uploads/2009/12/US-HLS-HLD-Structure-2010.pdf;
32. Internet Encyclopedia of Philosophy, "Hobbes: Moral and Political Philosophy", http://www.iep.utm.edu/hobmoral/;
33. Moir Anne, Jessel David, "Brain Sex", 1989;
34. "Amdocs Survey: Consumers Will Share Personal Data… at a Price", http://www.amdocs.com/News/Pages/amdocs-personal-data-consumer-survey.aspx;

35. Harris Michal, "Looking Through the PRISM: Three Customer Data Lessons", http://blogs.amdocs.com/insightfuel/2013/06/20/looking-through-the-prism-three-customer-data-lessons/;
36. Jonsher, Charles, "Wired Life, Who Are We in the Digital Age?", 1999;
37. Rezende Pedro A. D., "A Seita do Santo Byte", http://www.cic.unb.br/~rezende/trabs/azeredo.htm;
38. Kaiser Tiffany, "EU Investigates Microsoft for Policy Changes in Hotmail, Bing", http://www.dailytech.com/EU+Investigates+Microsoft+for+Policy+Changes+in+Hotmail+Bing/article29462.htm;
39. OECD (2013), "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value", OECD Digital Economy Papers, No. 220, OECD Publishing, http://dx.doi.org/10.1787/5k486qtxldmq-en;
40. "Panopticlick. How Unique – and trackable – is your browser", https://panopticlick.eff.org/;
41. Assolini Fabio, Kaspersky Lab, "Massive DNS poisoning attacks in Brazil", de 7 de novembro de 2011, http://www.securelist.com/en/blog/208193214/;
42. Nohl Karsten, "The DNS Operations, Analysis, and Research Center (DNS-OARC), a presentação da University of Virginia de 2008 https://www.dns-oarc.net/files/dnsops-2008/Nohl-DNS-privacy.pdf;
43. Mitnick Kevin, "A Arte de Enganar", edição brasileira Makron Books, 2003;
44. Diretiva 2006/24/CE do Parlamento e Conselho Europeus, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicação eletrônica publicamente disponíveis ou de redes públicas de comunicação, e que altera a Diretiva 2002/58/CE.
45. Kristol D. (Bell Laboratories, Lucent Technologies), Montulli L., (Netscape Communications), Request for Comments 2109, HTTP State Management Mechanism. Network Working Group, fevereiro de 1997, http://www.ietf.org/rfc/rfc2109.txt;
46. Kristol D. (Bell Laboratories, Lucent Technologies), Montulli L. (Epinions.com, Inc.), Request for Comments 2965, HTTP State Management Mechanism. Network Working Group, outubro de 2000, http://www.ietf.org/rfc/rfc2965.txt;
47. Miyazaki Anthony D. "Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage". 2008, American Marketing Association, Vol. 27 (1) Spring 2008;
48. Wikipédia inglesa, artigo "Evercookie", http://en.wikipedia.org/wiki/Evercookie;
49. Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:pt:HTML;
50. Microsoft Support, "INFO: Internet Explorer Does Not Send Referer Header in Unsecured Situations" http://support.microsoft.com/kb/178066;
51. Wikipédia inglesa, artigo "Usage share of web browsers", http://en.wikipedia.org/wiki/Usage_share_of_web_browsers;
52. MetaFilter, http://www.metafilter.com/95152/Userdriven-discontent#3256046
53. Wikipédia portuguesa, artigo "Gerenciadores de senhas", http://pt.wikipedia.org/wiki/Gerenciadores_de_senhas
54. Wikipédia inglesa, artigo "Password manager", http://en.wikipedia.org/wiki/Password_manager;
55. Reed Brad, BGR News para Yahoo News! 450,000 Yahoo passwords just got hacked; find out if you might be affected, de 12 de julho de 2012, http://news.yahoo.com/450-000-yahoo-passwords-just-got-hacked-might-155505616.html;
56. BBC NEWS Technology de 6 de junho de 2012, http://www.bbc.co.uk/news/technology-18338956;
57. Wing Kosner Anthony, "Unbelievable: Top Ten Hacked LinkedIn Passwords", Forbes, 6 de novembro de 2012, http://www.forbes.com/sites/anthonykosner/2012/06/11/unbelievable-top-10-hacked-linkedin-passwords/;
58. Smith Richard M., "The Web Bug FAQ" - http://w2.eff.org/Privacy/Marketing/web_bug.html;
59. Bailey, Oberheide, Andersen, Mao, Jahanian, Nazario, "Automated Classification and Analysis of Internet Malware"; Departamento da Engenharia Elétrica e Ciência da Computação da Universidade de Michigan, EUA, http://www.symantec.com/threatreport/;
60. Kaspersky Lab, http://www.kaspersky.com/about/news/press/2012/Android_Under_Attack__Malware_Levels_for_Googles_OS_Rise_Threefold_in_Q2_2012.
61. Netgear Procecure. Threat Monitor Virus.MSWord.Beast, http://prosecure.netgear.com/resources/threat-monitor-detail/Virus.MSWord.Beast?page=188;
62. Wikipédia inglesa, artigo "Suxnet", http://en.wikipedia.org/wiki/Stuxnet;
63. SpectorSoft, http://www.spectorsoft.com;

64. Bright Peter, "Microsoft Buys Skype for $8.5 Billion. Why, Exactly?", Wired, 10 de maio de 2011, http://www.wired.com/business/2011/05/microsoft-buys-skype-2/;
65. Godin Dan, ArsTechnica, "Think your Skype messages get end-to-end encryption? Think again", 20 de maio de 2013, http://arstechnica.com/security/2013/05/think-your-skype-messages-get-end-to-end-encryption-think-again/;
66. Wikipédia inglesa, artigo "Google China", http://en.wikipedia.org/wiki/Google_China;
67. The Telegraf, "Russian security service wants to ban Skype and Gmail" de 8 de abril de 2011, http://www.telegraph.co.uk/news/worldnews/europe/russia/8438617/Russian-security-service-wants-to-ban-Skype-and-Gmail.html;
68. Nilsen Thomas, Barents Observer, "FSB can tap your Skype without court order", de 14 de março de 2013, http://barentsobserver.com/en/security/2013/03/fsb-can-tap-your-skype-without-court-order-14-03;
69. Mather Tim, Kumaraswamy Subra, Latif Shahed,"Cloud Security and Privacy", O'Reilly, 2009;
70. Wikipédia inglesa, artigo"Criticism of advertising", http://en.wikipedia.org/wiki/Criticism_of_advertising;
71. Godin Seth. "Permission Marketing: turning strangers into friends, and friends into customers", 1999.
72. Fournier Susan, Dobscha Susan, Mick David Glen, "Preventing the Premature Death of Relationship Marketing", Harvard Business Review, janeiro-fevereiro de 1998;
73. Turow, Joseph, King, Jennifer, Hoofnagle, Chris Jay, Bleakley, Amy and Hennessy, Michael, Americans Reject Tailored Advertising and Three Activities that Enable It (September 29, 2009), SSRN, http://ssrn.com/abstract=1478214 ou http://dx.doi.org/10.2139/ssrn.1478214;
74. Wikipédia inglesa, artigo "Ad serving", https://en.wikipedia.org/wiki/Ad_serving;
75. Ferry Kate, Ad News, "Anúncio falso no Facebook comprova eficácia da rede social" http://www.adnews.com.br/publicidade/anuncio-falso-no-facebook-comprova-eficacia-da-rede-social;
76. Wikipédia inglesa, artigo "List of Google products" http://en.wikipedia.org/wiki/List_of_Google_services_and_tools;
77. Wikipédia inglesa, artigo "Electronic colonialism", http://en.wikipedia.org/wiki/Electronic_colonialism;
78. Farber Dan, "Facebook Colonizing the Internet", CBS News, http://www.cbsnews.com/8301-501465_162-20023480-501465.html;
79. Wikipédia inglesa, artigo "Criticism of Google", https://en.wikipedia.org/wiki/Criticism_of_Google;
80. Lars Reppesgaard, "Imperium Google" (título original: "Das Google-Imeprium", de 2008), edicação polonesa de 2009;
81. Google Investor Relations, http://investor.google.com/earnings/2012/Q4_google_earnings.html;
82. Facebook Newsroom, https://newsroom.fb.com/Key-Facts;
83. Megan Meier Foundation, http://meganmeierfoundation.org/megansStory.php;
84. The Tyler Clementi Foundation, http://www.tylerclementi.org/tylers-story/;
85. Ng Christina, ABC News, "Bullied Teen Amanda Todd's Death Under Investigation", http://abcnews.go.com/US/bullied-teen-amanda-todds-death-investigation/story?id=17489034;
86. Goldman Russell, ABC News, "Teens Indicted After Allegedly Taunting Girl Who Hanged Herself", http://abcnews.go.com/Technology/TheLaw/teens-charged-bullying-mass-girl-kill/story?id=10231357#.UccNQcjLf9c;
87. Ryan's story, http://www.ryanpatrickhalligan.org/about/about.htm;
88. American Management Association, 2007 Electronic Monitoring & Surveillance Survey, http://press.amanet.org/press-releases/177/2007-electronic-monitoring-surveillance-survey/
89. Privacy Rights Clearinghouse, https://www.privacyrights.org/fs/fs7-work.htm#gps;
90. Office of the Privacy Commissioner of Canda, "Privacy in the Workplace", http://www.priv.gc.ca/resource/fs-fi/02_05_d_17_e.ASP;
91. Staff Monitoring Solutions, http://www.staffmonitoring.com/P32/monitoring.htm;
92. Rizzo Alana, Monteiro Tânia, O Estado de S. Paulo, "Abin monta rede para monitorar internet", http://www.estadao.com.br/noticias/cidades,abin-monta-rede-para-monitorar-internet,1044500,0.htm;
93. Wikipédia inglesa, artigo "Internet censorship in the People's Republic of China", http://en.wikipedia.org/wiki/Internet_censorship_in_the_People%27s_Republic_of_China;
94. Reportes Without Borders, "Internet Enemies Report 2012", http://march12.rsf.org/i/Report_EnemiesoftheInternet_2012.pdf;
95. Wikileaks.org, http://www.wikileaks.org;
96. Edward Snowden Interview Transcript FULL TEXT: Read the Guardian's Entire Interview With the

Man Who Leaked PRISM, The Guardian e The Washington Post, 6 de junho de 2013, http://www.policymic.com/articles/47355/edward-snowden-interview-transcript-full-text-read-the-guardian-s-entire-interview-with-the-man-who-leaked-prism;
97. Wikipédia inglesa, artigo "Predictions of Soviet collapse", http://en.wikipedia.org/wiki/Predictions_of_Soviet_collapse;
98. Reporters Without Borders, "Enemies of the Internet 2013", http://surveillance.rsf.org/en/wp-content/uploads/sites/2/2013/03/enemies-of-the-internet_2013.pdf;
99. NSA Press Release de 24 de junho de 2010, "Declassified UKUSA Signals Intelligence Agreement Documents Available", http://www.nsa.gov/public_info/press_room/2010/ukusa.shtml;
100. European Parliament, "Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))", 11 de julho de 2001, http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A5-2001-0264&language=ET;
101. Greenwald Glenn, "Edward Snowden: the whistleblower behind the NSA surveillance revelations", http://www.guardian.co.uk/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance;
102. TechCrunch.com, "Google, Facebook, Dropbox, Yahoo, Microsoft, Paltalk, AOL And Apple Deny Participation In NSA PRISM Surveillance Program", http://techcrunch.com/2013/06/06/google-facebook-apple-deny-participation-in-nsa-prism-program/;
103. BBS News, "Joint EU-US group to assess US spy ops", http://www.bbc.co.uk/news/world-europe-23165257;
104. Código Penal Brasileiro de 1940, Artigo 299;
105. The United States Departent of Justice, http://www.justice.gov/criminal/fraud/websites/idtheft.html;
106. Identity Theft Resource Center, http://www.idtheftcenter.org/;
107. Bureau of Justice Statistics, "Identity Theft Reported by Households, 2005-2010", http://www.bjs.gov/index.cfm?ty=pbdetail&iid=2207;
108. id:analytics. "Identities of Nearly 2.5 Million Deceased Americans Misused Each Year", http://www.idanalytics.com/news-and-events/news-releases/2012/4-23-2012.php;
109. Declaração Universal Dos Direitos Humanos Adotada e proclamada pela resolução 217 A (III) da Assembléia Geral das Nações Unidas em 10 de dezembro de 1948, http://portal.mj.gov.br/sedh/ct/legis_intern/ddh_bib_inter_universal.htm;
110. Convenção Europeia dos Direitos do Homem, http://www.echr.coe.int/Documents/Convention_POR.pdf;
111. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part2;
112. Rule J.B., Greenleaf G., "Global Privacy Protection, The First generation";
113. InformationShield, "International Privacy Laws", http://www.informationshield.com/intprivacylaws.html;
114. Macrakis Kristie, "Seduced by Secrets: Inside the Stasi's Spy-Tech World";
115. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, Jornal Oficial nº L 281 de 23/11/1995 p. 0031 – 0050, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:PT:HTML;
116. Europa, Sínteses da legislação da UE, http://europa.eu/legislation_summaries/information_society/data_protection/l14012_pt.htm;
117. Parlamento Européu, Birô de Informações na Polônia, http://www.europarl.pl/pl/Aktualnosci_i_zaproszenia/Aktualnosci/news/news-2013/news_2013_June/ulotka_ochrona_prywatnosci_2013.html;jsessionid=269EA3CA15B934EEDC749636BE82444A;
118. Vincent J., Independent, "EU court rules in Google's favour: 'right to be forgotten' vetoed", http://www.independent.co.uk/news/world/europe/eu-court-rules-in-googles-favour-right-to-be-forgotten-vetoed-8672512.html;
119. Wikipédia inglesa, artigo "General Data Protection Regulation", http://en.wikipedia.org/wiki/General_Data_Protection_Regulationwikipedia.org;
120. Wikipédia inglesa, artigo " Personal Information Protection and Electronic Documents Act", http://en.wikipedia.org/wiki/Personal_Information_Protection_and_Electronic_Documents_Act;
121. export.gov, http://export.gov/safeharbor/
122. European Commision, Justice, http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/sec-2002-196/sec-2002-196_en.pdf;
123. European Commision, Justice, http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/sec-2004-

1323_en.pdf;
124. Connolly Chris (Galexia), "Privacy Laws and Business International", issue 96, December 2008; http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf;
125. InformationShield, http://www.informationshield.com/usprivacylaws.html;
126. Wikipédia inglesa, artigo "Brave New World", http://en.wikipedia.org/wiki/Brave_New_World;
127. Wikipédia inglesa, artigo "Brave New World Revisited" de 1958, (http://www.huxley.net/bnw-revisited/);
128. Wikipédia inglesa, artigo "Island (novel)" de 1962, http://en.wikipedia.org/wiki/Island_%28novel%29;
129. Slemmons Stratford Jean, Stratford Juri, "Data Protection and Privacy in the United States and Europe", www.iassistdata.org/downloads/iqvol223stratford.pdf;
130. Fleischer Peter: Privacy...?, "We Need a Better, Simpler Narrative of US Privacy Laws", de 12 de março de 2013, http://peterfleischer.blogspot.com/2013/03/we-need-better-simpler-narrative-of-us.html;
131. International Data Protection and Privacy Law - White & Case, http://www.whitecase.com/files/Publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/Presentation/PublicationAttachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_IntlDataProtectionandPrivacyLaw_v5.pdf;
132. InsidePrivacy, "China Releases National Standard for Personal Information Collected Over Information Systems; Industry Self-Regulatory Organization Established", de 25 de janeiro de 2013, http://www.insideprivacy.com/international/china-releases-national-standard-for-personal-information-collected-over-information-systems-industr/;
133. The Economist, "The long march to privacy", http://www.economist.com/node/5389362 (carregado em 6 de julho de 2013);
134. Making Sense of China's New Privacy Laws, The Hogan Lovells Privacy Team, de 28 de junho de 2013, https://www.privacyassociation.org/privacy_tracker/post/making_sense_of_chinas_new_privacy_laws;
135. Wikipédia russa, artigo: "Федеральный закон «О персональных данных»", http://ru.wikipedia.org/wiki/ Федеральный_закон_«О_персональных_данных»;
136. Wikipédia russa, artigo: "Оператор персональных данных", http://ru.wikipedia.org/wiki/Оператор_персональных_данных (carregado em 6 de julho de 2013);
137. Wikipédia inglesa, artigo: " Data protection (privacy) laws in Russia ",http://en.wikipedia.org/wiki/Data_protection_%28privacy%29_laws_in_Russia;
138. Алексей Королюк (Aleksey Koroliuk), CNews, Эксперты: закон «О персональных данных» нужно доработать, de 30 de junho de 2011, http://internet.cnews.ru/news/line/index.shtml?2011/06/30/445794;
139. Wikipédia portuguesa, artigo "Marco Civil da Internet", http://pt.wikipedia.org/wiki/Marco_Civil_da_Internet;
140. Campi M., Info Online, "Brasil é o 4ª principal alvo de roubo de dados online", de 10 de junho de 2013, http://info.abril.com.br/noticias/seguranca/brasil-e-o-4-principal-alvo-de-roubo-de-dados-online-10062013-21.shl;
141. Chade J., ESTADÃO.COM.BR/Internacional, "Brasil é o 3º país que mais pede dados ao Google", http://www.estadao.com.br/noticias/impresso,brasil-e-o-3-pais-que-mais-pede-dados-ao-google-,1040131,0.htm;
142. B. Tavares, C. Stanisci, R. Burgarelli e B. Boghossian, ESTADÃO.COM.BR, "Informação pessoal vale R$ 100", de 19 de agosto de 2010, http://blogs.estadao.com.br/jt-seguranca/tag/comercio/page/2/;
143. Wikipédia inglesa, artigo "Pretty Good Privacy", https://en.wikipedia.org/wiki/Pretty_Good_Privacy;
144. Wikipédia inglesa, artigo "Tor (anonimity network)", https://en.wikipedia.org/wiki/Tor_%28anonymity_network%29;
145. TrackMeNot, http://cs.nyu.edu/trackmenot/;
146. Microsoft, Central da Proteção e Segurança, "Ajude a proteger crianças online: 4 coisas que você pode fazer", http://www.microsoft.com/pt-br/security/family-safety/childsafety-steps.aspxç
147. Wikipédia inglesa, artigo: Panpticon", http://en.wikipedia.org/wiki/Pan-ópticoç
148. Wikipédia inglesa, artigo: "Panopticism", http://en.wikipedia.org/wiki/Panopticism".