SOCIEDADE EM REDE, INTERNET E ESTADO DE VIGILÂNCIA: ALGUMAS APROXIMAÇÕES

NETWORK SOCIETY, INTERNET AND STATE OF SURVEILLANCE: SOME APPROACHES

Carlos Alberto Molinaro[1]
Professor da PUCRS

Ingo Wolfgang Sarlet[2]
Professor Titular da PUCRS

RESUMO: A utilização crescente das tecnologias invasivas nas comunicações sociais de qualquer tipo ameaça remodelar nossas expectativas de liberdade e privacidade nas esferas públicas e, notadamente, nos espaços privados. Essas tecnologias são capazes de gravar grandes quantidades de dados pessoais de forma eficiente e sem precedentes. Nesse contexto, é possível falar de um novo modelo de colonização produzido por essas tecnologias de espionagem explícita. Outra significativa ameaça à liberdade e à privacidade é a compilação massiva de dados pessoais por organizações privadas. Essa informação muitas vezes move-se através de "fluxos de informação legal" que têm por objeto o auxílio em investigações criminais, e, sob esse argumento, muitas vezes as empresas privadas divulgam indevidamente coleções de dados pessoais, incluindo despesas de cartão de crédito, registros telefônicos, hábitos de navegação na Web, *e-mail*, registros e transações financeiras. Neste cenário, o sistema jurídico deve responder de modo eficiente na proteção à liberdade e à privacidade, especialmente com um robusto instrumental legal que garanta a integridade do direito à informação e à comunicação.

---

1 Doutor em Direito (Universidade Pablo de Olavide, Sevilha, com menção Europeia). *Site*: www.camolinaro.net.

2 Doutor e Pós-Doutor em Direito (Ludwig-Maximilians-Universität-München), Juiz de Direito no Rio Grande do Sul, Brasil.

PALAVRAS-CHAVE: Estado de vigilância; Internet e intrusão; liberdade e privacidade.

ABSTRACT: *The increasing use of intrusive technologies in social communications of any type threatens reshape our expectations of freedom and privacy in public spheres and notably in private spaces. These technologies are able to store large amounts of personal data efficiently and in a manner without precedent. We are facing a new model of colonization produced by these explicit espionage technologies. Another significant threat to liberty and to privacy is the massive compilation of personal data by private organizations. This information often moves through "legal information flows" which have the object the aid in criminal investigations, and under that argument, often private companies improperly disclose personal data collections including credit card expenses, phone records, and web browsing habits, e-mail records and financial transactions. In this scenario, the legal system must respond effectively to protecting liberty and privacy, especially with robust legal instruments guaranteeing the integrity of the right to information and communication.*

KEYWORDS: *Surveillance state; internet and intrusion; privacy and liberty.*

1 OBSERVAÇÕES INICIAIS

O termo *Sociedade em Rede* (*Network Society*) foi originalmente cunhado pelo Professor norueguês Stein Bråten, em 1981, no seu *Modeller av menneske og samfunn: bro mellom teori og erfaring fra sosiologi og sosialpsykologi* (*Modelos do ser humano e da sociedade: a ponte entre a teoria e a experiência, da sociologia e psicologia social*)[3], tendo sido retomado mais tarde (1991) pelo Professor holandês Jan Van Dijk na obra *De Netwerkmaatschappij, sociale aspecten van nieuwe media* (*A Sociedade em Rede, aspectos sociais da nova*

[3] A referência está na obra publicada em inglês, por Stein Bråten, *Roots and Collapse of Empathy: Human nature at its best and at its worst* (Amsterdam: John Benjamins Publishing, 2013. p. 115 e ss.).

mídia)[4]. Posteriormente, a mesma expressão foi utilizada, em 1996, por Manuel Castells[5] e, a partir daí, passou a ser amplamente difundida.

As inúmeras tipificações atribuídas ao modelo social da atualidade podem gerar, aos desavisados, alguma perplexidade quanto a sua significação ou identificação. Neste ensaio adotamos a denominação Sociedade em Rede, vinculando-a, também, a um novo modelo de Estado, o assim designado *Estado de Vigilância*, uma forma de contaminação da democracia caracterizada pela intrusão dos governos e das corporações na liberdade e na privacidade de terceiros, sejam estes atores públicos ou privados. Todavia, quando falamos em sociedade em rede não desprezamos aquela atribuição típica: Sociedade da Informação (ou do Conhecimento)[6]. Nesse sentido, no conceito de uma "sociedade da informação", o que é enfatizado é a substancial e sempre presente

---

4 Jan Van Dijk, publicou em inglês a 2ª edição deste livro, *The Network Society, Social Aspects of New Media*. Há uma terceira edição ampliada em 2012 (London: Sage), a qual tivemos acesso. A Sociedade em Rede, como Van Dijk a vê, pode explicar um novo tipo de sociedade onde as relações sociais são organizadas no âmbito de tecnologias mediáticas que formam uma rede de comunicação em vez de redes tipificadas pelas relações sociais face-a-face. Esta lógica organizacional diferente dá origem a diferentes capacidades das unidades sociais e que as sociedades anteriores não podiam alcançar. Ele diferencia a sociedade em rede da sociedade da informação: o conceito de sociedade da informação concentra-se na substancial transformação dos processos sociais, enquanto o conceito de sociedade em rede examina as formas de organização dos processos sociais.

5 Manuel Casttels, *The Rise of the Network Society: the Information Age: Economy, Society and Culture* (2. ed., with a new preface first published 2010), 1º volume da trilogia *The Information Age: Economy, Society, and Culture* (Oxfordo: John Wiley & Sons, 2010). Pode-se obter uma cópia deste livro (edição de 2010 em inglês) na página Web do Professor Deniz Yengin, coordenador de Communication Design – Multimedia da Istanbul Kultur University – Faculty of Art and Design (http://www.denizyengin.com/dy/yabancikaynak_files/TheRise%20ofTheNetworkSociety.pdf). Não sabemos se tal reprodução foi autorizada, mas, por tratar-se de acadêmico com referência internacional, acreditamos que tenham sido respeitados os direitos autorais respectivos; há tradução para o português de Roneide Venâncio Majer (*A sociedade em rede*. 6. ed. São Paulo: Paz e Terra, v. 1, 1999 (13. reimp., 2010).

6 A chamada Sociedade da Informação é caracterizada por um conjunto de pressupostos, perfeitamente legítimos para a Europa, os Estados Unidos e o Japão, não o sendo, no entanto, para a maioria dos outros países fora dessas áreas de influência. Basicamente, esta sociedade da informação, definida como a terceira revolução (ou a terceira onda, palavras de Toffler), e também como "era da comunicação", é caracterizado por três pilares: (a) a existência de um novo modelo cultural, (b) uma mudança permanente e vertiginosa dos sistemas, (c) a mistura de interesses econômicos e políticos. Por razões sistemáticas, podemos dizer que esta nova sociedade da informação tem características específicas, incluindo: (1) o grande quantidade de informações, (2) a informação instantânea, (3) a organização bipolar da informação, (4) os sistemas interativos de informação, (5) a inovação tecnológica constante, (6) em formato digital (7), a onipresença da Internet. Consequentemente, pode-se descrever a quantidade de fontes de informação, a diversidade e as estratégias para a divulgação das mesmas, levando a uma enorme quantidade de informação em bruto ou trabalhada (refinada) que nenhum ser humano, individualmente, tem a capacidade integral acedê-las. Atualmente, temos mais

transformação das atividades e dos processos ocorrentes no interior dessas sociedades, baseadas na ciência, racionalidade e reflexividade. Uma sociedade cuja economia e em geral todos os valores e setores, inclusive os setores agrários, industriais e de serviços, está caracterizada cada vez mais pela produção de informação. O mercado de trabalho caracteriza-se por uma maioria de funções largamente ou completamente baseada em tarefas de processamento de informação que requerem conhecimento e níveis mais elevados de ensino (daí a atribuição: sociedade do conhecimento). A cultura, por sua vez, é dominada pela mídia e pelos produtos de informação com os seus sinais, símbolos e significados[7]. De outra parte, no conceito de uma "sociedade em rede", a atenção desloca-se para as formas de organização dessa sociedade, examinando as mutações de sua infraestrutura. O conceito de "sociedade em rede" enfatiza a forma, o intercâmbio e a organização do processamento de informação. Uma infraestrutura das redes sociais e da mídia se encarrega disso. Assim, a sociedade em rede pode ser definida como uma formação social com uma infraestrutura de redes sociais e meios de comunicação que permitam o seu modo principal de organização em todos os níveis (individual, grupal/organizacional e social). Cada vez mais, essas redes permitem vincular todas as unidades ou partes desta formação (indivíduos, grupos e organizações). Nas sociedades ocidentais, o "indivíduo vinculado por redes" está se tornando a "unidade básica" da sociedade em rede. Nas sociedades orientais, ao contrário, ainda é o grupo (família, comunidade, trabalho em equipe) que está vinculado por redes[8]. Em ambas, como anota Van Dijk, "[...] as redes atendem todos os níveis da sociedade e se conectam nestes níveis. A Internet, por exemplo. Simultaneamente atende aos indivíduos, as organizações, as comunidades e sociedades. Nunca tivemos tal meio na história antes"[9].

Vale observar que a análise de Van Dijk evita os tons excessivamente deterministas de Castells, pois sua abordagem moderada vê as redes organizadas de acordo com os seus níveis (bióticos e abióticos), mas cada nível

capacidade de escolher a informação, mas o que realmente importa é a possibilidade de aceder com qualidade à informação.

7 Cf. VAN DIJK, Jan. *The Network Society, Social Aspects of New Media*. 3. ed. London: Sage, 2012. p. 23.

8 Cf. VAN DIJK, Jan. *The Network Society, Social Aspects of New Media*. 3. ed. London: Sage, 2012. p. 24 e, notadamente, p. 48.

9 "*Currently, networks serve at every level of society and they connect these levels. The Internet, for example. Simultaneously serves individuals, organizations, communities and societies. We have never had such a medium in history before.*" (Op. cit., loc. cit).

é dinamicamente inter-relacionado no contexto do que ele denomina de "modo de organização hierárquica", muito embora tais níveis, inferiores e superiores, sejam "codeterminados". Em contraste com Castells, Van Dijk é a favor, para análise desses fenômenos, da manutenção de unidades sociais do tipo individual, familiar e organização. Um dos pontos interessantes desenvolvidos por Van Dijk é a sua explicação para o aparente aumento da individualização, que se revela evidente nas sociedades modernas de alta tecnologia. Neste contexto, ele vê a ascensão do individualismo como um contraponto à crescente penetração da rede, ou seja, o nivelamento em termos de acessibilidade para cada indivíduo conectado em uma rede. A uniformidade potencial, ainda que soe paradoxal, leva a uma demanda social para o indivíduo se diferenciar. Com efeito, embora estejamos todos no *Facebook*, cada página é única, mas se trata, ao fim e ao cabo, de um modelo de generalização e padronização do ambiente social para atender as tendências opostas de particularidade e diferenciação cultural[10]. Esses dois conceitos, "sociedade em rede" e "sociedade da informação", se complementam e, para a sua caracterização, podemos dizer, que se exigem reciprocamente.

Esse novo modelo de sociedade (em rede, da informação e do conhecimento) está submetido aos mais diversificados engenhos de controle e intrusão, ainda que se possa afirmar que tal fenômeno (controle e intrusão) não seja novo, mas que assumiu formas e proporções substancialmente novas e intensivas no contexto da sociedade em rede. Note-se, nessa perspectiva, que mesmo os Estados de Direito (democráticos), com destaque para os ocidentais, exercem entre si – segundo os interesses políticos e econômicos por eles apreciáveis – uma competição cada vez mais intensa relativamente ao "domínio da informação"[11]. A informação, de outro modo, tem se constituído, no cenário global, como uma poderosa e eficiente nova forma de "escambo" e, como tal, sem equivalência direta em termos de valor. Todavia, poucos são os Estados com suficiente "capital informacional", e, por isso mesmo, são eles que dominam esse "novo mercado", gerando uma nova modalidade de hegemonia. Estado de vigilância[12], tem sido

[10] Aut. cit., op. cit., p. 175.

[11] Por certo, os regimes autocráticos sempre foram os vilões da história no que diz com o exercício dominante da vigilância, mas eles não são os únicos governos que intensificaram suas atividades de fiscalização. Podemos dizer, mesmo, que os contemporâneos Estados Democráticos, de algum modo, copiaram e copiam, e em certa medida, as práticas intrusivas daqueles.

[12] Cf. a obra do festejado sociólogo belga Armand Mattelart, *La globalisation de la surveillance. Aux origines de l'ordre sécuritaire* (Paris: La Découverte, 2007), em inglês, a que tivemos acesso, *Globalization of Surveillance* (Cambridge-UK: Polity Press, 2010), onde o autor afirma que o terrorismo é percebido como uma ameaça global, e a busca da segurança passa a ser um processo contagioso transcendendo

a "alcunha" deferida à forma pela qual se exerce o poder pela informação, ao passo que o modo pelo qual se interage nesse mercado se revela no e por meio de um "governo vigilante". A guerra contra o terror pode ser a justificativa mais familiar para o surgimento do Estado de Vigilância, mas não é a única, sequer sendo a causa mais importante. O uso crescente do "governo de vigilância" e a prática da "mineração" de dados constituem um resultado previsível, tendo em conta a acelerada evolução no campo da tecnologia da informação. Com as cada vez mais poderosas tecnologias que nos permitem descobrir e analisar o que está acontecendo no mundo, os governos e as entidades privadas adquirem maior influência e poder. A questão não é mais se vamos ter um "Estado de vigilância" (assim como um "estado de vigilância"[13]) nos próximos anos, mas que tipo de Estado será este. Será que vamos ter um governo sem controles suficientes sobre a vigilância pública e privada, ou será que teremos um governo que protege a dignidade individual e que está em conformidade com as exigências do Estado de Direito? Nesse contexto, não se pode negligenciar o fato de que no Estado de Vigilância, a linha entre as esferas pública e privada de policiamento e segurança estão esvanecidas, se não totalmente inexistentes, pois o público e o privado estão inteiramente conectados e imbricados[14]. Assim, à vista de tais considerações introdutórias e tendo em conta que o nosso intento é o de analisar como o Estado de Vigilância impacta os direitos fundamentais, com destaque para a liberdade e privacidade dos indivíduos, nada melhor do

as fronteiras nacionais e atribuindo as agências internacionais, cada vez mais poderosas, "um mandato de busca de segurança". Nesse processo, os dados do cidadão perdem a sua proteção, interligando-os livremente com a inclinação generalizada de priorizar a segurança sobre os direitos individuais. O autor explora a rastreabilidade dos indivíduos e das *commodities* em todas as esferas da vida com base no rápido avanço dos dispositivos tecnológicos. Esse novo recurso do contexto global atual é a capacidade crescente de tecnologias de vigilância e identificação. Essas tecnologias são capazes de alterar a relação de poder entre o Estado e as corporações globais operadas pelo setor privado. Em contraste com a inovação das tecnologias militares, baseadas no financiamento público e dirigidas pelo Estado, mas é a demanda global do setor empresarial que impulsiona a inovação de vigilância e tecnologia de identificação. Mattelart aponta para a dinâmica do mercado na área de perfis comerciais, com base em RFID (dispositivo de identificação por rádio frequência), e os registros de cartões de crédito, entre outros, e em que medida ela está a ponto de adquirir dimensões orwellianas. Mattelart refere-se às redes paralelas de vigilância no setor privado, notadamente nas relações laborais e de serviços. Alerta que a combinação da utilidade de vigilância abrangente e a identificação biométrica para o mundo corporativo e o enfraquecimento regulador do Estado na esteira da economia neoliberal, sugere que a esfera pessoal é severamente ameaçada pela espionagem corporativa (p. 32, 49 e ss., p. 117 e ss., especialmente p. 183 e ss.).

13 Além da figura do Estado como tal, também se verifica um estado no sentido de uma situação, condição, na qual se encontram os Estados enquanto unidades políticas e as sociedades.

14 Cf. Robert O'Harrow Jr., *No Place to Hide* (New York: Free Press, 2006. p. 27, 160, 166, 241).

que iniciar com uma sumária apresentação dos contornos principais desse novo modelo de Estado, para, na sequência, adentrar a problemática da proteção dos direitos fundamentais.

2 O ASSIM CHAMADO ESTADO DE VIGILÂNCIA E SEUS TRAÇOS ESSENCIAIS

Conforme já referida, a guerra contra o terror pode ser (especialmente desde o fatídico 11 de Setembro de 2001) a justificativa mais familiar para o surgimento do Estado de Vigilância, mas seguramente não se trata nem da única razão ou mesmo da razão mais importante. O uso crescente do Governo de Vigilância e da "Mineração de Dados" é, como igualmente já destacado, o resultado previsível da evolução acelerada da tecnologia da informação, pois se trata de tecnologias que nos permitem descobrir e analisar o que está acontecendo no mundo, cuidando-se de ferramentas cada vez mais utilizadas pelos Estados e mesmo por atores sociais não estatais, mais ou menos poderosos. No "Estado Nacional de Vigilância"[15], o "governo usa a vigilância", a mineração de dados, o seu agrupamento e a sua respectiva análise para identificar e evitar potenciais ameaças, mas, também, para melhor administrar e prestar serviços sociais. O Estado de vigilância, como anota Balkin, é um caso especial de "Estado de Informação" (erigido sobre uma Sociedade da Informação), um Estado que intenta identificar e resolver problemas de governança por meio da coleção, do agrupamento, da análise e da produção de informação[16].

Na ambiência desse modelo de Estado, o ponto de ruptura entre a liberdade e a segurança reside na privacidade, especialmente por causa da perplexidade e da incerteza crescente em virtude das ameaças do terrorismo e do incremento em termos quantitativos e qualitativos das transgressões ocorrentes na Rede (o espaço amplo do cibercrime), fatos que têm estimulado as restrições (e violações) dos direitos individuais, afrontando a vida privada em particular. O ponto de ruptura, a privacidade, encontra-se, portanto, em permanente estado de vigilância, em geral arbitrária. A vigilância passa a operar como atividade e

[15] Cf. Jack M. Balkin, The Constitution in the National Surveillance State (2008). Faculty Scholarship Series. Paper 225. Disponível em: <http://digitalcommons.law.yale.edu/fss_papers/225>. Acesso em: 15 out. 2013. Neste artigo, o Professor Balkin, pela primeira vez, cunha a expressão "National Surveillance State", identificando dois tipos de Estado de Vigilância, primeiro é um Estado de Vigilância autoritário, enquanto o segundo é um Estado de Vigilância democrático. E os recentes escândalos (cf. toda a celeuma em torno de Edward Snowden) revelam claramente que vivemos em um autoritário.

[16] Cf. Jack M. Balkin, Op. cit., loc. cit., p. 3.

modo de perquirição (e perseguição) sistemático e metódico, compreendendo o monitoramento de ações ou comunicações de uma ou mais pessoas, instituições privadas e públicas e mesmo dos Estados. Uma revivescência do panóptico benthamiano, mais sofisticado e intrusivo, ou uma nova visão do mesmo em Foucault[17], onde se fazem presentes, entre outras, pelo menos uma ou mais ações, combinadas ou não: (a) vigilância do comportamento; (b) vigilância das comunicações; (c) vigilância de dados (e intercepção); (d) vigilância de localização e rastreamento; (e) vigilância do corpo (biométrica).

A pergunta que não quer calar, e que tem ocupado lugar central no debate político, jurídico, sociológico e filosófico atual, é se nesse modelo de Estado (da Vigilância) ainda há lugar para um sistema de direitos humanos e de direitos fundamentais, ou, pelo menos, se há como assegurar a tais direitos humanos e fundamentais condições mínimas de efetividade. Por certo, o problema reside em dar efetividade aos direitos, evitando ou reprimindo ações que envolvam o observar, o ocultar, o espiar, ou o espreitar por parte desse Estado, especialmente naquilo em que tais ações frequentemente e muitas vezes de forma silenciosa afetam os direitos fundamentais.

A Constituição brasileira, em vigor desde 5 de outubro de 1988, molda o perfil jurídico-político do País, e caracteriza-se por sua forma rígida, organizando um Estado Democrático de Direito, em uma República Federativa formada pela união indissolúvel dos Estados, dos Municípios e do Distrito Federal. A Constituição da República acolhe, promove e garante a liberdade de expressão, a liberdade de imprensa e o direito à informação (art. 5º, IV IX e XIV; e art. 220 da CF/1988), de um lado, e o direito à privacidade (art. 5º, X, da CF/1988), de outro. A garantia constitucional da liberdade de expressão, em todas as suas modalidades, e da privacidade, em todos os seus níveis de densidade, é uma exigência democrática e um imperativo associado à proteção dos direitos humanos e fundamentais albergados na Constituição. Assim como o fez o Brasil, a maioria dos Estados de Direito contemporâneos (assim como o sistema internacional e regional de proteção dos direitos humanos) acolhe esses direitos

[17] Michel Foucault, *Discipline and Punish* (London: Penguin, 1977). Para Foucault, o Panopticon era uma metáfora que permitia explorar a relação entre: a) sistemas de controle social e as pessoas em uma situação disciplinar; e b) o conceito de "conhecimento é poder". Na sua opinião, o poder e o conhecimento vem da observação de outras pessoas. Ele marcou a transição para um poder disciplinar, com todos os movimentos supervisionado e todos os eventos gravados. O resultado desta vigilância é a aceitação das normas e a docilidade de comportamento – uma "normalização das sortes", decorrente da ameaça de disciplinamento (p. 77).

na condição de expressão máxima de todo e qualquer regime que se pretenda democrático[18].

[18] Cf., por exemplo, a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (CEDH), art. 10º: "Liberdade de expressão – 1. Qualquer pessoa tem direito à liberdade de expressão. Este direito compreende a liberdade de opinião e a liberdade de receber ou de transmitir informações ou ideias sem que possa haver ingerência de quaisquer autoridades públicas e sem considerações de fronteiras. O presente artigo não impede que os Estados submetam as empresas de radiodifusão, de cinematografia ou de televisão a um regime de autorização prévia. 2. O exercício desta liberdades, porquanto implica deveres e responsabilidades, pode ser submetido a certas formalidades, condições, restrições ou sanções, previstas pela lei, que constituam providências necessárias, numa sociedade democrática, para a segurança nacional, a integridade territorial ou a segurança pública, a defesa da ordem e a prevenção do crime, a proteção da saúde ou da moral, a proteção da honra ou dos direitos de outrem, para impedir a divulgação de informações confidenciais, ou para garantir a autoridade e a imparcialidade do poder judicial". A Carta dos Direitos Fundamentais da União Europeia, art. 11º: "Liberdade de expressão e de informação – 1. Todas as pessoas têm direito à liberdade de expressão. Este direito compreende a liberdade de opinião e a liberdade de receber e de transmitir informações ou ideias, sem que possa haver ingerência de quaisquer poderes públicos e sem consideração de fronteiras. 2. São respeitados a liberdade e o pluralismo dos meios de comunicação social". Nas Constituições: Alemanha: "*Article 5 [freedom of expression, arts and sciences] (1) Every person shall have the right freely to express and disseminate his opinions in speech, writing and pictures, and to inform himself without hindrance from generally accessible sources. Freedom of the press and freedom of reporting by means of broadcasts and films shall be guaranteed. There shall be no censorship. (2) These rights shall find their limits in the provisions of general laws, in provisions for the protection of young persons, and in the right to personal honour. (3) Arts and sciences, research and teaching shall be free. The freedom of teaching shall not release any person from allegiance to the constitution*". Itália: "*Art. 21 Anyone has the right to freely express their thoughts in speech, writing, or any other form of communication. The press may not be subjected to any authorization or censorship. Seizure may be permitted only by judicial order stating the reason and only for offences expressly determined by the law on the press or in case of violation of the obligation to identify the persons responsible for such offences. In such cases, when there is absolute urgency and timely intervention of the Judiciary is not possible, a periodical may be confiscated by the criminal police, which shall immediately and in no case later than 24 hours refer the matter to the Judiciary for validation. In default of such validation in the following 24 hours, the measure shall be revoked and considered null and void. The law may introduce general provisions for the disclosure of financial sources of periodical publications. Publications, performances, and other exhibits offensive to public morality shall be prohibited. Measures of preventive and repressive measure against such violations shall be established by law*". Japão: "*Article 21. Freedom of assembly and association as well as speech, press and all other forms of expression are guaranteed. No censorship shall be maintained, nor shall the secrecy of any means of communication be violated*". México: "*Article 6. The expression of ideas shall not be subject to any judicial or administrative investigation unless such expression offends good morals, infringes upon the rights of others, incites crime, or disturbs the public order; the right to a reply shall be exercised subjects to the terms established by law. Freedom of information shall be guaranteed by the State. With regard to the exercise of the right of access to information, the Federation, the State, and the Federal District shall act, within their respective competences, in accordance with the following principles and basic tenets: I – Any information held by any federal, State or municipal authority, entity, organ or body is public and may be held back only temporarily for public interest reasons in accordance with the terms established by law. II – Information relating to private life and personal data shall be protected in the terms and with the exceptions provided for by law. III – Everybody shall have free access to public information, his/her personal data or the correction of the latter, without having to show any cause or justification for their use. IV – Mechanisms for granting access to*

information and speedy correction procedures shall be established. Those procedures shall be conducted before specialized and impartial organs and bodies enjoying autonomy in terms of operation, management and decision-making. V – The persons and institutions subject to the [previously defined] obligations shall keep their records in updated public registries and shall publish via the available electronic media the complete and updated information about their management indicators and the use of public funds. VI – The laws shall determine the manner in which the persons and institutions subject to the [previously defined] obligations shall make public the information concerning the public funds which they transmit to individuals and juridical persons. VII – The non-compliance with provisions concerning the access to public information shall be sanctioned in the conditions defined by the laws". Portugal: "*Article 37. Freedom of expression and information – 1. Everyone shall possess the right to freely express and publicize his thoughts in words, images or by any other means, as well as the right to inform others, inform himself and be informed without hindrance or discrimination. 2. Exercise of the said rights shall not be hindered or limited by any type or form of censorship. 3. Infractions committed in the exercise of the said rights shall be subject to the general principles of the criminal law or the law governing administrative offences, and shall be brought before the courts of law or an independent administrative body respectively, as laid down by law. 4. Every person and body corporate shall be equally and effectively guaranteed the right of reply and to make corrections, as well as the right to compensation for damages suffered. Article 38. Freedom of the press and the media. 1. The freedom of the press shall be guaranteed. 2. Freedom of the press shall mean: a) Journalists and other staff's freedom of expression and creativity, as well as journalists' freedom to take part in determining the editorial policy of the media body in question, save when it is doctrinal or denominational in nature; b) Journalists' right, as laid down by law, to gain access to sources of information and to the protection of professional independence and secrecy, as well as their right to elect editorial boards; c) The right to found newspapers and any other publications, regardless of any prior administrative authorization, bond or qualification. 3. In generic terms, the law shall ensure that the names of the owners of media bodies and the means by which those bodies are financed are publicized. 4. The state shall ensure the media's freedom and independence from political power and economic power by imposing the principle of specialization on businesses that own general information media, treating and supporting them in a non-discriminatory manner and preventing their concentration, particularly by means of multiple or interlocking interests. 5. The state shall ensure the existence and operation of a public radio and television service. 6. The structure and operation of public sector media shall safeguard their independence from the Government, the Public Administration and the other public authorities, and shall ensure that all the different currents of opinion are able to express themselves and to confront one another. 7. Radio and television broadcasting stations shall only operate with licenses that are granted under public calls for tender, as laid down by law. Article 39. Regulation of the media. 1. An independent administrative body shall be responsible for ensuring the following in the media: a) The right to information and the freedom of the press; b) The non-concentration of ownership of the media; c) Independence from political power and economic power; d) Respect for personal rights, freedoms and guarantees; e) Respect for the statutes and rules that regulate the work of the media; f) That all different currents of opinion are able to express themselves and confront one another; g) Exercise of the rights to broadcasting time, of reply and of political response. 2. The law shall define the composition, responsibilities, organization and modus operandi of the body referred to in the previous paragraph, together with the status and role of its members, who shall be appointed by the Assembly of the Republic and co-opted by those so appointed. Article 40. Right to broadcasting time, of reply and of political response. 1. Political parties, trade unions, professional and business organizations and other organizations with a national scope shall, in accordance with their size and representatives and with objective criteria that shall be defined by law, possess the right to broadcasting time on the public radio and television service. 2. Political parties that hold one or more seats in the Assembly of the Republic and do not form part of the Government shall, as laid down by law, possess the right to broadcasting time on the public radio and television service, which shall be apportioned in accordance with each party's proportional share of the seats in the Assembly, as well as to reply or respond politically to the Government's political statements. Such times shall be of the same duration and prominence as those given over to the Government's broadcasts and statements. Parties with seats in the*

À vista desse quadro, as práticas intrusivas, seja àquelas praticadas pelos Estados nacionais, seja as levadas a efeito pelos setores privados, atentam contra os princípios democráticos, violando em muitos casos os direitos (humanos e fundamentais). Chama a atenção, nesse contexto, que na atualidade as afrontas aos direitos de privacidade e liberdade acabam por vir especialmente daqueles Estados que sempre ostentaram a condição de constituírem democracias de alta densidade, caso típico dos Estados Unidos da América e da Grã-Bretanha, entre poucos outros. De outra parte, o conjunto normativo (nacional e internacional) consagrado, e que intenta proteger a liberdade de expressão e a privacidade, não consegue lograr os seus fins, padecendo de um défice generalizado de eficácia, seja por falta de vontade política, seja em virtude das externalidades econômico-financeiras. O recente (17.04.2013) Informe de Frank La Rue[19] delineia uma série de inquietudes em virtude da multiplicação de novos instrumentos de vigilância programados para infiltrarem-se nos dispositivos informáticos de qualquer tipo e em alguns casos "[...] rastrear e registrar as comunicações de Internet e de telefonia em escala nacional"[20]. La Rue anota que as tecnologias de vigilância estão sendo multiplicadas e são cada vez mais sofisticadas. Como resultado disso, "[...] o Estado tem agora, como nunca antes observado, uma maior capacidade de levar a cabo a vigilância simultânea, invasiva, específica e de ampla escala"[21], e acrescenta:

> Tecnologias de vigilância modernas e convênios que permitem aos Estados intrometerem-se na vida privada do indivíduo ameaçam obscurecer a divisão entre as esferas privada e pública. Elas facilitam a monitorização

Legislative Assemblies of the autonomous regions shall enjoy the same rights within the ambit of the region in question. 3. During elections and as laid down by law, candidates shall possess the right to regular and equitable broadcasting time on radio and television stations with a national or regional scope" (Cf., o excelente Projeto Constitute, The World's Constitutions to Read, Search, and Compare. Disponível em: <https://www.constituteproject.org/#/>).

19 Relator Especial para a promoção e proteção do direito de liberdade de opinião e de expressão (*Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*) das Nacões Unidas.

20 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue: "*Today, some States have the capability to track and record Internet and telephone communications on a national scale*" (p. 11). Disponível em: <http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf>. Acesso em: 23 maio 2013.

21 "[...] *the State now has a greater capability to conduct simultaneous, invasive, targeted, and broad-scale surveillance than ever before*." (p. 10 – Frank La Rue, loc. cit.).

> invasiva e arbitrária dos indivíduos, que podem não ser capazes de sequer saber que foram submetidos a esse tipo de vigilância, muito menos desafiá-la. Os avanços tecnológicos significam que a efetividade do Estado na condução de vigilância não é mais limitada pela escala ou duração.[22]

O Relator é enfático ao dizer que aos governos incube tomar medidas "para impedir a comercialização de tecnologias de vigilância"[23], criticando as empresas que têm desenvolvido tecnologias que permitem a vigilância massiva, mediante a violação do direito à intimidade consagrado na Declaração Universal dos Direitos Humanos e nas diversas ordens jurídicas (pelo menos boa parte das ocidentais) democráticas contemporâneas. Ele afirma que a interceptação das comunicações pode estar justificada pela necessidade de identificar os criminosos, mas as leis nacionais que regulam a vigilância nas comunicações são, de regra, "inadequados ou inexistentes"[24]. La Rue adverte que esta propensão deve ser alterada, pois os governos deveriam atualizar suas leis para "garantir que os direitos humanos sejam respeitados e protegidos", e a guarda dos dados dos usuários pelas empresas, com fins de vigilância, deveria ser proibida. Espionagem, afirma o Relator, "só deve ser produzida em circunstâncias excepcionais". Vigilância deve ser supervisionada por uma autoridade independente, e os governos devem ser "plenamente transparentes"

---

22 "*Modern surveillance technologies and arrangements that enable States to intrude into an individual's private life threaten to blur the divide between the private and the public spheres. They facilitate invasive and arbitrary monitoring of individuals, who may not be able to even know they have been subjected to such surveillance, let alone challenge it. Technological advancements mean that the State's effectiveness in conducting surveillance is no longer limited by scale or duration*." (p. 10 – Frank La Rue, loc. cit.).

23 "[...] *to prevent the commercialization of surveillance technologies*." (p. 22 – Frank La Rue, loc. cit.).

24 "*Concerns about national security and criminal activity may justify the exceptional use of communications surveillance technologies. However, national laws regulating what would constitute the necessary, legitimate and proportional State involvement in communications surveillance are often inadequate or non-existent. Inadequate national legal frameworks create a fertile ground for arbitrary and unlawful infringements of the right to privacy in communications and, consequently, also threaten the protection of the right to freedom of opinion and expression*." (As preocupações sobre a segurança nacional e a atividade criminal pode justificar o uso excepcional das tecnologias de vigilância de comunicações. No entanto, as leis nacionais que regulam o que constituiria o necessário, envolvimento legítimo e proporcional do Estado na vigilância das comunicações são muitas vezes inadequadas ou inexistentes. Quadros jurídicos nacionais inadequados criam um terreno fértil para uma ilegal e o arbitraria violação ao direito à privacidade nas comunicações e, consequentemente, também ameaçam a proteção do direito à liberdade de opinião e de expressão) (Frank La Rue, loc. cit., p. 3)

no que diz com suas técnicas de vigilância e os poderes que utilizam[25]. Todavia, os fatos recentemente divulgados amplamente pela mídia internacional e local (por exemplo, os que envolveram o escândalo com o ex-agente da CIA Edward Snowden) demonstram o quão pouco é provável que as recomendações de La Rue sejam adotadas no marco da política de qualquer governo a curto prazo, já que as medidas por ele apontadas não têm caráter vinculativo e servem basicamente para assessorar aos Estados-membros da ONU.

Assim, o que se percebe é que o assim chamado Estado de Vigilância, ainda que nas vestes de Estado Democrático de Direito, representa uma realidade a ser compreendida, analisada e confrontada, especialmente naquilo em que arrosta direitos fundamentais e direitos humanos tão duramente conquistados ao longo de tanto tempo. Este, contudo, é o objeto do próximo item.

3 INTERNET, LIBERDADE DE EXPRESSÃO E PRIVACIDADE – AMEAÇAS E DESAFIOS

Anteriormente, já anotamos que "a privacidade não é apenas uma importante demarcação, um limite legítimo à liberdade de expressão, mas sim, que a privacidade é também uma condição para a liberdade de expressão, sendo ambas indispensáveis para a plena participação numa sociedade democrática". A liberdade de expressão e a privacidade podem – em determinadas circunstâncias – significar considerações desiguais para pessoas desiguais. Novas tecnologias quase sempre afetam a nossa liberdade de expressão e a nossa privacidade. Navegação GPS, cartões inteligentes, pedágios eletrônicos em transportes, câmeras públicas, inquéritos eletrônicos, *scanners* fixos ou móveis em qualquer lugar, todos de algum modo afetam a nossa liberdade e privacidade. Nesse

[25] "*Communications surveillance should be regarded as a highly intrusive act that potentially interferes with the rights to freedom of expression and privacy and threatens the foundations of a democratic society. Legislation must stipulate that State surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority. Safeguards must be articulated in law relating to the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law.*" (A vigilância nas comunicações deve ser considerada como um ato altamente intrusivo que, potencialmente, interfere com os direitos à liberdade de expressão e privacidade, e ameaçam as bases de uma sociedade democrática. A legislação deve estipular que a vigilância Estado nas comunicações só deve ocorrer nas circunstâncias mais excepcionais e exclusivamente sob a supervisão de uma autoridade judicial independente. Salvaguardas devem ser articuladas em legislação, relativa à natureza, âmbito e duração das medidas possíveis, bem como os fundamentos necessários para requisitá-la, as autoridades competentes para as autorizar, realizar e supervisionar, e o tipo de recurso previsto pela legislação nacional) (Frank La Rue, loc. cit., p. 21)

contexto, sabemos que todo e qualquer acesso à Internet deixa rastros que podem ser seguidos e monitorados, permitindo o compartilhamento e repasse de informações, em geral sem a correspondente autorização de seu titular. Ainda que isso pareça não ser objeto de preocupação por muitas pessoas, que inclusive espontaneamente se expõe de diversas formas na Rede, o fato é que há quem prefira ter sua privacidade preservada, gerando, assim, um problema em termos de proteção de diversos direitos fundamentais.

Na atual quadra, cabe especialmente ao internauta a iniciativa para proteger-se. Todavia, o melhor que pode fazer – e isso não garante absoluto anonimato – é ativar a função de navegação privada/não me sigas (*do not track*) do navegador Web[26]. A verdade é que o cenário de ampla intrusão que se verifica especialmente na Internet ofusca cada vez mais a democracia, o Estado de Direito e os direitos humanos e fundamentais, visto que cada vez é maior o acesso irrestrito dos governos e de seus diversos órgãos (e, mesmo, de corporações privadas de diferenciado tipo) às nossas informações pessoais, que acabam por ser absorvidas por grupos de interesse e poder que ainda não conhecemos bem, e cujo objetivo é o da construção de um "campo de informação mundial" uniforme e o aperfeiçoamento dos processos de informação com distintos fins. Tudo isso está em um simples "*click*" (!)[27].

Com efeito, o periódico britânico *The Guardian* tem publicado, desde algum tempo, ampla matéria sobre as mais recentes intromissões e manipulações de dados por agências de espionagem norte-americanas e britânicas, a *National Security Agency* (NSA) e a *Government Communications Headquarters* (GCHQ)[28],

---

[26] GARFINKEL, Simson. *Database Nation*: The Death of Privacy in the 21st Century. Sebastopol-CA: O'Reilly Media Inc., 2001. p. 257 y ss.

[27] Observe-se que a Agência de Segurança Nacional dos Estados Unidos tem a capacidade de bisbilhotar em quase todas as comunicações enviadas a partir de um Apple iPhone, de acordo com documentos vazados compartilhados pelo pesquisador de segurança Jacob Appelbaum em *Der Spiegel*. Disponível em: <http://www.spiegel.de/netzwelt/netzpolitik/neue-dokumente-der-geheime-werkzeugkasten-der-nsa-a-941153.html>. Acesso em: 30 dez. 2013.

[28] Em 5 de junho (2013), *The Guardian* publica sua primeira exclusiva entrevista com Edward Snowden, denunciante da NSA, revelando que o governo dos EE.UU obrigou a gigante das telecomunicações VERIZON a entregar os registros telefônicos de milhões de estadunidenses; em 6 de junho, revelou a existência do programa PRISM, na edição de junho dá notícia do software *Boundless Informant* (Informante sem limites) – que permite gravar e analisar a proveniência dos dados (Disponível em: <http://www.guardian.co.uk/world/the-nsa-files>). Nas edições de 21 e 22 de junho, o periódico revelou as intromissões na comunicação de dados pela GCHQ (Disponível em: <http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>; <http://www.guardian.co.uk/uk/2013/jun/23/mi5-feared-gchq-went-too-far>).

mediante a utilização de programas como PRISM e TEMPORA, respectivamente[29]. Contudo, não foram somente essas agências, na atualidade o Serviço Federal de Inteligência da Alemanha (*Bundesnachrichtendienst* – BND) entra no jogo anunciando querer estender o controle sobre a Internet massivamente. Segundo a informação veiculada pelo *site Spiegel Online*, cerca de 100 milhões de euros seriam investidos nos próximos cinco anos no departamento de "educação técnica" da agência para ampliar seu pessoal e equipamento[30]. Não bastassem esses fatos, também cooperam para o obscurecimento da Web os instrumentos legislativos nacionais e internacionais que intentam vigiar, manipular e violar os já debilíssimos sistemas de segurança de dados mediados na Rede. Vejam-se os malogrados ensaios, como SOPA, PIPA e ACTA. Os denominados projetos norte-americanos PIPA e SOPA (United States House of Representatives # 3261/2011, e United States Senate # 968/2011) tinham por objetivo estabelecer uma forma sofisticada para controlar a transmissão e o intercambio da informação gerada por e na Internet. O primeiro, de iniciativa do Senado dos Estados Unidos, o PROTECT IP Act, ou *Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011* (PIPA, de acordo com a sigla em inglês)[31], de autoria do Senador Patrick Leahy, e o segundo, *Stop Online Piracy Act* (SOPA em inglês)[32], de autoria do Deputado Lamar Smith, ambos os projetos foram arquivados em 18.01.2012 e 20.01.2012, respectivamente, como consequência dos protestos da cidadania e das instituições da sociedade civil.

O projeto europeu ACTA – *Anti-Counterfeiting Trade Agreement*[33] foi instituído com grande discrição, quase secretamente, provando ser controvertido desde o dia em que foi proposto pela primeira vez. Com tal projeto, intentava-se dar maior eficácia na aplicação dos direitos de propriedade intelectual em âmbito internacional, mas, no bojo do projeto, um modelo sofisticado do SOPA tentou impor novas sanções e medidas tendentes a "compelir" os usuários da Internet a "cooperar" com a indústria do entretenimento, para vigiar e censurar as comunicações em linha por cima da autoridade judicial penal. O projeto

29 Disponível em: <http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>. Acesso em: 22 jun. 2013.

30 Cf., edição de 17 jun. 2013. Disponível em: <http://www.spiegel.de/politik/deutschland/ueberwachung-fdp-kritisiert-spionage-plaene-des-bnd-scharf-a-906078.html>.

31 Disponível em: <http://www.govtrack.us/congress/bills/112/s968>. Acesso em: 23 jan. 2012.

32 Para maiores detalhes, disponível em: <http://judiciary.house.gov/hearings/pdf/112%20HR%203261.pdf> e <http://www.judiciary.house.gov/issues/Rogue%20Websites/Summary%20Manager's%20Amendment.pdf>. Acesso em: 30 fev. 2013.

33 Para ler na íntegra o projeto em vinte e dois idiomas: http://bit.ly/xPDyNj.

representou uma grave ameaça para a liberdade de expressão na Internet, além de criar grande insegurança jurídica para os usuários da Rede. O ACTA enfrentou uma forte oposição por parte da cidadania europeia que o vê como antidemocrático. Muitos saíram às ruas em um protesto sincronizado, afirmando que o ACTA viola os seus direitos. Umas 200 cidades participaram da "marcha contra o ACTA" em fevereiro de 2012[34], e, em 4 de julho de 2012, o Parlamento Europeu rechaçou o acordo em sessão plenária com 479 votos contra o tratado, 39 votos a favor e 165 abstenções de deputados do Parlamento Europeu[35].

Enquanto toda a atenção centrava-se no SOPA, no PIPA e no ACTA (os assim denominados projetos de lei contra a pirataria na Internet), uma nova peça legislativa surge ainda mais controvertida, designadamente, o *Cyber Intelligence Sharing and Protection Act* (CISPA), aprovada pela Câmara de Representantes (Assembleia dos Deputados) dos Estados Unidos em 18.04.2013. O projeto de lei foi aprovado por uma votação de 248 votos a favor e 168 contrários, com maioria de votos de representantes republicanos[36]. Os defensores do projeto afirmam que o intercâmbio de informações permitiria ao governo e às agências de segurança conhecer, controlar e combater as ameaças detectadas na Rede. Com o CISPA, o governo poderia compartir essas ameaças com as empresas privadas e ajudar na proteção de suas Redes, assim como as empresas compartiriam suas informações (e as de seus usuários) com o governo e suas agências[37], uma promiscuidade intolerável se confrontada com os princípios democráticos e com os direitos humanos e fundamentais da cidadania. O projeto depende do Senado norte-americano, com maioria democrática. Esse já se pronunciou no sentido de rechaçar o projeto como está, tendo sido oferecido pelo presidente do Comitê de Comércio do Senado projeto de lei de segurança cibernética. Se a emenda conseguir sobreviver ao processo de aprovação do *Cybersecurity Act*, pode finalmente tornar-se lei. Note-se que o substitutivo foi aprovado por

---

34 Disponível em: <https://www.accessnow.org/blog/acta-protest-feb-11>. Acesso em: 3 mar. 2012.

35 Disponível em: <https://www.accessnow.org/policy/internet-governance-reform>. Acesso em: 23 ago. 2012.

36 Nada obstante a petição com mais de 800.000 assinaturas, dirigida ao Congresso norte-americano, lançada em 5 de abril de 2012 por Avaaz.org (https://secure.avaaz.org/en/), uma plataforma *on-line* para organização cívica, ela descreve o CISPA como um projeto de lei "que daria às empresas privadas e do governo dos EUA o direito de espionar qualquer um de nós a qualquer momento, durante o tempo que quiserem sem um mandado" (Petição disponível em: <https://secure.avaaz.org/en/stop_cispa/>).

37 Cf., Huffington Post, edição de 12 abr. /2013. Disponível em: <http://www.huffingtonpost.com/2013/04/18/cispa-vote-house-approves_n_3109504.html>.

unanimidade pela Comissão de Comércio em julho de 2013, mas encontra-se parado desde então[38].

Todavia, tudo isso não é novo! As revelações de Edward Snowden ao *The Guardian*[39] apenas confirmam o que Perry Fellwock (também um ex--analista da NSA) havia denunciado 42 anos atrás: o amplo programa de espionagem da NSA[40]. O estudo, elaborado por Duncan Campbell para o *European Parliament's Directorate-General for Research*, dava conta de que a vigilância eletrônica pelo Estado dos anos 1970/1990 era realizada por meio da Inteligência de Comunicações (COMINT), ou seja, mediante a busca automática de comunicações eletrônicas que possibilitava a interceptação global de tais comunicações[41]. Observe-se, ainda, que, em 1988, Campbell advertia:

> Agências de inteligência americana, britânica e aliados estão prestes a embarcar em uma expansão maciça, bilhões de dólares de seu sistema de vigilância eletrônica global. De acordo com informação dada recentemente em segredo para o Congresso dos EUA, o sistema de vigilância permitirá que as agências monitorem e analisem as comunicações civis no século XXI. Identificado no momento como projeto P415, o sistema será executado pela NSA. Mas as agências de inteligência de muitos outros países estarão intimamente envolvidas com a nova rede, incluindo os da Grã-Bretanha, Austrália, Alemanha e Japão e, surpreendentemente, a República Popular da China.[42]

---

38 *Site* oficial do Senado Norte-americano. Disponível em: <http://beta.congress.gov/bill/113th/senate-bill/1353/committees>. Acesso em: 12 dez. 2013. Também o texto disponível em: <http://beta.congress.gov/113/bills/s1353/BILLS-113s1353is.xml>. Acesso em: 12. dez. 2013.

39 Entrevista em The Guardian. Disponível em: <http://www.theguardian.com/theguardian/2013/jun/10>.

40 A entrevista com Perry Fellwock pode ser acessada no sita de CRYPTONE (http://cryptome.org/), que reproduz a publicação em Ramparts, v. 11, n. 2, p. 35-50, aug. 1972: U.S. Electronic Espionage: A Memoir (Disponível em: <http://cryptome.org/jya/nsa-elint.htm>. Acesso em: 23 mar. 2012). Também no *site* de WikiLeaks (Disponível em: <http://wikileaks.org/wiki/Perry_Fellwock>).

41 Disponível em: <http://aei.pitt.edu/41012/1/Development.of.surveillance.Vols.1-5.pdf>. Acesso em: 2 mar. 2012.

42 "*American, British and Allied intelligence agencies are soon to embark on a massive, billion-dollar expansion of their global electronic surveillance system. According to information given recently in secret to the US Congress, the surveillance system will enable the agencies to monitor and analyze civilian communications into the 21st century. Identified for the moment as Project P415, the system will be run by the US National*

Em 1996, Nicky Hager publicou seu *Secret Power: New Zealand's Role in the International Spy Network*[43], onde descreve em detalhe o Projeto ECHELON (já denunciado por Perry Fellwock e Duncan Campbell). Segundo o autor, o original ECHELON remonta a 1947, quando, como resultado da cooperação em época de guerra, o Reino Unido e os Estados Unidos concordaram em continuar, em âmbito mundial, as atividades de "inteligência de comunicação" (COMINT[44]). Os dois países deveriam trabalhar juntos para estabelecer um sistema global de interceptação, sempre que possível, uma vez que partilhavam o equipamento especial necessário para essa finalidade, bem como com as despesas necessárias e, um e outro, teriam o acesso aos resultados. Posteriormente, Canadá, Austrália e Nova Zelândia juntaram-se ao denominado acordo UKUSA[45]. Hager demonstra e conclui que a interceptação (atual) de comunicações por satélite é o núcleo do atual sistema. Desde o final de 1990, três denunciantes, todos bem conhecidos da NSA (Bill Binney, J. Kirk Wiebe e Tom Drake), revelaram os intentos invasivos

Security Agency (NSA). But the intelligence agencies of many other countries will be closely involved with the new network, including those from Britain, Australia, Germany and Japan, surprisingly, the People's Republic of China". O texto na íntegra está Disponível em: <http://www.duncancampbell.org/menu/journalism/newstatesman/newstatesman1988/They've%20got%20it%20taped.pdf> (página do autor). Foi publicado em New Statesman, de 12 ago. 1988, p. 10/12. Também pode ser lido no *site*: http://cryptome.info/echelon-dc.htm (acesso em: 6 fev. 2012).

43 Publicado por Nelson (NZ: Craig Potton Publishing, 1996).

44 COMINT ou "comunicações de inteligência", inclui-se nos serviços de inteligência adquirido através da intercepção de comunicações estrangeiras, excluindo as emissões de rádio e televisão abertas. É um subconjunto de inteligência de sinais, ou SIGINT, com o último sendo entendido como compreendendo COMINT e ELINT, inteligência eletrônica, derivada da não comunicação de sinais eletrônicos tais como radar. Durante a primeira parte da época moderna de "inteligência", os termos "inteligência de sinais" e "inteligência de comunicações" foram usados permutável e virtualmente, e, portanto, muito do que foi descrito como sinais de inteligência durante a segunda guerra mundial é mais corretamente entendido como COMINT. Cf., *International Electronic Countermeasures*, editado pelo Journal of Electronic Defense (Norwood/MA: Horizon House Publications Inc., 2004, p. 6, 13, e 20). Para aprofundamento também confira o excelente trabalho de Frederick D. Parker, *Pearl Harbor Revisited: U.S. Navy Communications Intelligence 1924-1941*, publicação distribuída livremente pela NSA, com nota de advertência de que ela não reflete, necessariamente, a posição da NSA/CSS, ou qualquer outra entidade do governo dos EUA (Disponível em: <http://www.nsa.gov/about/_files/cryptologic_heritage/publications/wwii/pearl_harbor_revisited.pdf>. Acesso em: 15 dez. 2013).

45 Segundo Antonio Miguel Molina Molina e Antonio Javier Tallón Ballesteros, em *Privacidad de la información: espionaje personal* (Proyecto Fin de Carrera. Universidad de Granada. E. T. S. I. Informática. Diciembre 2004) UKUSA "*es una organización constituida por los siguientes Estados: los Estados Unidos y el Reino Unido principalmente y, dentro de las posibilidades de cada uno, Australia, Canadá y Nueva Zelanda. Actualmente, UKUSA se ha apartado de su objetivo original de defensa, frente a las potencias del bloque del Pacto de Varsovia y China, y se le supone dedicada a la lucha antiterrorista y contra el narcotráfico, aunque existen contundentes pruebas de que también se dedica al espionaje económico. ECHELON no es más que una herramienta de* UKUSA *para alcanzar sus oscuros objetivos*" (p. 93).

da Agência, informando ao Inspetor-Geral do Departamento de Defesa e, posteriormente, aos Comitês de Supervisão do Congresso dos Estados Unidos, que um programa multimilionário de recolecção de dados da NSA, conhecido como *Trailblazer*, foi ineficaz, o que representou enorme desperdício de recursos. Além disso, foi também denunciado o programa conhecido como *Stellar Wind*, destinado a bloquear procedimentos que impediam a aquisição dos dados dos cidadãos norte-americanos. Graças a esses cidadãos e outros (registre-se aqui o recente caso Snowden), sabemos que o governo norte-americano realiza intensa vigilância social (em seu território e alhures), monopolizando dados, utilizando para tanto diferenciado instrumental informático, além de obter dados das corporações, das redes sociais, dos buscadores de Internet, inclusive das redes de telefonia móvel, tudo a configurar uma ampla rede de vigilância e intrusão na esfera das relações sociais e dos interesses e direitos individuais e coletivos.

Como se pode perceber, as ameaças e os desafios à liberdade e à privacidade (na Rede e em todos os ambientes onde se processam relações socioculturais e econômicas) estão e sempre estiveram presentes. Para fazer frente a essa situação, não basta pensar-se um "direito digital", mas sim, além disso, é necessário, como já frisado, caminhar com Hervé Fischer na articulação de uma perspectiva filosófica. Fischer acredita que a Internet representa um marco na história da humanidade, tão importante quanto a descoberta do fogo, sua aparição no silêncio, sua insídia, sua generalidade e seu radicalismo afetam todos os aspectos da atividade humana, de tal sorte que, de acordo com o autor, necessária a construção de uma "filosofia da cibernética" para lidar com esta nova realidade[46]. O fato é que em poucos anos construímos um dispositivo gigante com uma arquitetura muito complexa que pode armazenar e distribuir bilhões e bilhões de arquivos binários instantaneamente. Com efeito, *software*, roteadores, navegadores, motores de busca, agentes inteligentes e outros dispositivos produzem (e irão produzir), armazenam, enviam e baixam bilhões de páginas de informações e imagens de exibição, interligados pelos mais diferentes "portais". Este espaço, por outro lado, é sempre crescente e mutante, pois o seu desempenho e a sua velocidade estão aumentando exponencialmente, bem como a quantidade e qualidade das informações que nele são geradas e nele circulam. Este é o espaço que chamamos de "mundo cibernético"[47]. Através

[46] FISCHER, Hervé. *Digital Shock – Confronting the New Reality*. Quebec, Canada: McGill-Queen's University Press, 2006, p. VII e ss.

[47] FISCHER, Hervé. *Digital Shock – Confronting the New Reality*. Quebec, Canada: McGill-Queen's University Press, 2006, p. 43.

de suas estruturas e de seu conteúdo, o mundo cibernético reflete o mundo real de que é derivado. Mas o ciberespaço é mais, é um mundo paralelo e não simplesmente um espelho ou substituto do mundo. Porque, além de refletir o mundo real, o mundo cibernético se autogera de acordo com sua lógica e suas necessidades, com uma quantidade e qualidade cada vez maior de conteúdos inéditos, o que é "único" e que se liberta dos constrangimentos do mundo real. O ciberespaço tem sua própria dinâmica e cresce e se desenvolve com certa autonomia e com características que são muito diferentes do mundo real. O mundo cibernético é um reino imaginário, em que encontramos lógica, valores, conteúdos e comportamentos individuais e sociais, positivos e negativos, que são frequentemente muito diferentes daqueles que se encontram no mundo real. Assim, estabeleceu-se uma espécie de dialética entre dois universos paralelos, com base na fuga, na compensação complementar, na gestão, na exploração e na oposição, de tal sorte que estamos a vivenciar e participar de ambos os mundos, em uma mescla do real e do virtual[48]. Que tudo isso implica riscos é hoje algo incontroverso.

Embora não se trate de algo tão difundido, um dos maiores riscos em termos especialmente da afronta aos princípios democráticos e do seu potencial em termos de violação de direitos humanos e fundamentais encontra-se no denominado *Trans-Pacific Partnership Agreement* (TPPA ou TPP)[49], semelhante, mas muito mais intrusivo, do que os já referidos SOPA, CISPA ou ACTA. Nesse contexto, vale lembrar que o SOPA e o ACTA foram suspensos em grande parte em virtude das pressões exercidas pelo ativismo popular. O principal motivo

[48] Aut. cit., op. cit., p. 44 y ss.

[49] A Parceria Trans-Pacífico (TPP) transveste-se como um acordo de "livre comércio", com o objetivo de definir regras sobre questões comerciais e não comerciais, como a segurança alimentar, a liberdade na Internet, os preços dos medicamentos, a regulação financeira, e ao meio ambiente. Ela conforma um sistema de governança internacional vinculativo que exigiria dos Estados Unidos, Austrália, Brunei, Canadá, Chile, Japão, Malásia, México, Nova Zelândia, Peru, Singapura, Vietnã, e qualquer outro país que venha dela participar, adequar suas políticas nacionais com as suas regras, algumas delas que claramente violam elementares princípios da soberania dos Estados. Essa "parceria" tem sido negociada em segredo, e incluiu lideres político dos países participantes e mais de 600 agentes corporativos: "assessores comerciais oficiais", os textos gerados nas conferencias não estão ao alcance de membros dos parlamentos, da imprensa, da sociedade civil e do público. O material conhecido é resultante de vazamento na Internet, de denúncias de professores e ativistas dos direitos humanos e de alguma mídia comprometida com a defesa da liberdade de expressão e da privacidade. Cf., para o aprofundamento sobre o TPPA, de modo especial, o vinculado pelo *site* da WikiLeaks, uma organização de mídia sem fins lucrativos, disponível em: <http://wikileaks.org/tpp/>; também o *site* da Electronic Frontier Foundation (EFF), dedicado a defesa da liberdade na Rede, disponível em: <https://www.eff.org/issues/tpp>.

das pressões foi o fato, comum aos dois documentos, de que os detentores de direitos autorais teriam condições de forçar a sua vontade na Internet, por exemplo, mediante a responsabilização dos internautas responsáveis pela infração de conteúdos protegidos, inclusive permitindo a suspenção das contas de Internet de infratores reincidentes. Análise acadêmica mais detalhada do capítulo referente à propriedade intelectual (Capítulo 10) desse novo arranjo internacional está emergindo após o vazamento de um documento de 95 páginas pelo WikiLeaks[50]. A análise do capítulo TPP/IP (capítulo sobre propriedade intelectual[51]) fornecido pelo WikiLeaks mostra que ele está seguindo um caminho semelhante, mas potencialmente até mesmo mais intrusivo e despótico do que se verificaria no caso de aprovação do ACTA. Isso levou a comunidade acadêmica, em vários países, a se manifestar contra o acordo. Nesse sentido, uma carta de 80 professores de Direito de prestigiadas Escolas nos Estados Unidos foi dirigida ao parlamento e ao presidente do País, exortando preocupações e alertando que

> o TPP está seguindo um processo ainda mais secreto do que o ACTA, que está ampliando a desconfiança do público e criando um ambiente propício para um produto final desequilibrado e indefensável, [...] em vez de repetir os fracassos do ACTA, os Estados Unidos devem seguir o exemplo do último sucesso internacional alcançado com o Tratado de Marrakesh[52], exemplo de transparência sem precedentes para um acordo internacional[53].

---

50 O documento poder ser obtido por *download*, disponível em: <https://wikileaks.org/tpp/static/pdf/Wikileaks-secret-TPP-treaty-IP-chapter.pdf>. Acesso em: 14 dez. 2013.

51 Sobre este capítulo, os autores do presente ensaio estão preparando artigo exclusivo, com análise e exame dogmático de suas inferências, a ser publicado brevemente.

52 O Tratado de Marrakech, recentemente adotado pela Organização Mundial da Propriedade Intelectual (OMPI) permite o acesso a obras publicadas para os cegos, deficientes visuais ou outras dificuldades acessando texto impresso, torna-se uma ferramenta para a educação e cultura. Sobre o Marrakesh Treaty to Facilitate Access to Published Works by Visually Impaired Persons and Persons with Print Disabilities (Disponível em: <http://www.wipo.int/dc2013/en/>).

53 Na íntegra, disponível em: <http://infojustice.org/wp-content/uploads/2013/11/Law-Professors-TPP-11142013.pdf>. Acesso em: 12 dez. 2013. Outras manifestações, inclusive a do Professor Joseph Stiglitz, podem ser acessadas em: http://keionline.org/sites/default/files/jstiglitzTPP.pdf; e http://english.agrinews.co.jp/?p=146. Confira ainda o excelente livro *Hacia una Internet libre de censura – Propuestas para América Latina* (Facultad de Derecho, Centro de Estudios en Libertad de Expresión y Acceso a la Información), organizado por Eduardo Bertoni e disponível em: <http://www.palermo.edu/cele/pdf/internet_libre_de_censura_libro.pdf>; bem como o artigo do Professor Neil M.

O capítulo relativo à propriedade intelectual acarreta profundas e substantivas mudanças no direito internacional, com reflexos acentuados nas ordens locais. Do texto vazado na Rede é possível identificar uma dura lei de direitos de autor, espelhada na dos Estados Unidos, e que teria o potencial de alterar as leis nacionais em toda a região. Caso o documento fosse aprovado e adotado no estado em que se encontra, sua articulação, impulsionada principalmente pelos EUA, implicaria padrões de proteção da propriedade intelectual mais rígidos e aplicáveis a todo e qualquer âmbito autoral. Ocorre que o documento reproduz partes do controverso ACTA, além de revitalizar alguns dispositivos do SOPA, alterando, assim, a capacidade de acessar informações e recursos vitais para países em desenvolvimento, tudo em sentido contrário ao que rezam acordos multilaterais mais transparentes e já celebrados, tais como Aspectos Relacionados ao Comércio da OMC e do Acordo de Direitos de Propriedade Intelectual (TRIPS). Em termos de direitos autorais, o TPP irá expandir drasticamente seus padrões mínimos internacionais em termos de duração. Em caráter ilustrativo, cabe referir que o tratado propõe estender o prazo dos direitos de autor sobre obras publicadas, que passariam a expirar 70 anos após a morte do autor ou não menos de 95 anos desde a primeira publicação autorizada. Isso iria aumentar a extensão de direitos autorais em uma parcela significativa dos países signatários, bem como anular o padrão TRIPS de 50 anos após a morte ou 50 anos após a sua publicação. Embora este período de *copyright* espelhe a lei dos EUA, a lei dos EUA estabelece 70 anos *post mortem* como um teto, enquanto o TPP adota tal critério como um referencial mínimo[54].

Nada obstante o TPP aborde uma gama de questões, onde se incluem inúmeras condições relativas às relações internacionais na perspectiva econômica, as negociações sempre foram e são realizadas de modo altamente sigiloso, pois as conferências foram realizadas a portas fechadas, revelando uma incrível falta de transparência. Assim, o que o Presidente Obama declarou como sendo o acordo do século XXI[55] parece inaugurar uma nova "era de segredo", em

Richards da Washington University School of Law, disponível em: <http://www.harvardlawreview.org/symposium/papers2012/richards.pdf>.

54 Cf., Sean M Flynn, Margot E. Kaminski, Brook K. Baker e Jimmy Koo, Public Interest Analysis of the US TPP Proposal for an IP Chapter (December 6, 2011). Northeastern University School of Law Research Paper, n. 82-2012; American University, WCL Research Paper, n. 2012-07. Available at SSRN: http://ssrn.com/abstract=1980173 or http://dx.doi.org/10.2139/ssrn.1980173 (acesso em> 13 maio 2013).

55 "*We, the Leaders of Australia, Brunei Darussalam, Chile, Malaysia, New Zealand, Peru, Singapore, United States, and Vietnam, are pleased to announce today the broad outlines of a Trans-Pacific Partnership (TPP)*

vários aspectos similar ao que se passou na assim chamada "Guerra Fria", pois o sigilo impede o diálogo entre o público em geral, bem como inibe o debate na esfera das organizações acadêmicas e mesmo políticas. Além disso, o crescente livre acesso aos meios de comunicação, especialmente o acesso à Internet, cada vez mais, dadas a circunstâncias já apontadas, gera uma ilusão de liberdade e ao mesmo tempo expõe a vida privada e os direitos de personalidade conexos a um cada vez maior número de ingerências e mesmo de violações, resultando em um défice preocupante de proteção de tais direitos. Mas isso será objeto de atenção mais detida em outro momento.

4 OBSERVAÇÕES FINAIS

Apesar do crescimento continuado do aparato social e da ampliação de seus campos de atuação, o Estado se encontra imerso em uma conjuntura de atuação cada vez mais condicionada; está condicionado e limitado por uma inovadora e complexa atuação da sociedade civil, na qual todos se incluem, e que se têm apoderado das decisões não reguladas pelo Estado. Por outro lado, o Estado encontra-se condicionado e limitado pela transnacionalização da vida econômica, cultural e social que se produziu nas últimas décadas, e que fez com que princípios e categorias sobre os quais se assentavam a organização e o exercício do poder político não possam mais ser considerados plenamente vigentes na atualidade. De outro modo, as grandes transformações

agreement among our nine countries. We are delighted to have achieved this milestone in our common vision to establish a comprehensive, next-generation regional agreement that liberalizes trade and investment and addresses new and traditional trade issues and 21st-century challenges. We are confident that this agreement will be a model for ambition for other free trade agreements in the future, forging close linkages among our economies, enhancing our competitiveness, benefitting our consumers and supporting the creation and retention of jobs, higher living standards, and the reduction of poverty in our countries." (Nós, os líderes da Austrália, Brunei, Chile, Malásia, Nova Zelândia, Peru, Singapura, Estados Unidos e Vietnã, temos o prazer de anunciar hoje as linhas gerais de um acordo de Parceria Trans-Pacífico (TPP) entre os nossos nove países. Estamos muito satisfeitos por ter alcançado este marco em nossa visão comum para estabelecer um acordo global, de próxima geração regional, que liberaliza o comércio e investimento e aborda questões de comércio, novas e tradicionais, e os desafios do século 21. Estamos confiantes de que este acordo será um modelo para a ambição de outros acordos de livre comércio no futuro, forjando ligações estreitas entre nossas economias, aumentando a nossa competitividade, beneficiando nossos consumidores e apoiando a criação e manutenção de postos de trabalho, padrões de vida mais elevados, bem como a redução da pobreza em nossos países). Essa parte do discurso está na página da Casa Branca) (Disponível em: <http://www.ustr.gov/about-us/press-office/press-releases/2011/november/trans-pacific-partnership-leaders-statement>. Acesso em: 10 jan. 2012)

tecnoeconômicas[56], o tecnotropismo[57], bem como as mudanças que se verificaram no domínio da informação incidiram nas relações de poder, que com isso sofreram uma importante e profunda mudança, implicando uma crise sem precedentes do Estado como entidade soberana. Não podemos esquecer que a democracia política, tal como a entendemos, se funda na ideia de Estado soberano, portanto, o que está em jogo hoje é a própria modelagem do processo democrático, já que a translineação das fronteiras da soberania conduz necessariamente a uma incerteza no processo de delegação da vontade dos cidadãos, agentes e atores sociais. A hipótese está na afirmação de que o Estado está envolvido internacionalmente em uma rede demasiadamente ampla para resolver pequenos problemas locais, e, por outro lado, frente à amplitude da rede internacional e dos fluxos transversais de poderes econômico-financeiros, científicos e tecnológicos o Estado é sempre demasiado pequeno para resolver os grandes problemas globais.

Nesse contexto, duas grandes variáveis devem ser observadas: de um lado, têm-se os problemas de sobrevivência (ecologia profunda, tensão entre as condicionantes da paz frente aos conflitos) que escapam do domínio e do controle dos Estados, assumindo outros agentes o encargo de assoalhar uma desestatização das relações internacionais. De outra parte, e como efeito direto da globalização da economia e das tecnologias de informação e comunicação (TIC), o Estado resultou muito acanhado para a solução dos problemas emergentes dessa nova realidade, e também muito rígido para controlar os fluxos globalizantes do poder político-financeiro. Daí abriga-se na "capa escura" da vigilância de todos (e de nenhum em particular, pois o que vigia está só).

Por outro lado, esse mesmo Estado (pelo menos naquilo que representa o modelo de um Estado Democrático de Direito) defronta-se com os novos desafios de uma sociedade em Rede, de uma sociedade da informação ou do

---

[56] A propósito a noção de "tecnoeconomia" está bem articulada no trabalho de Michel Callon (The dynamics of techno-economic networks, in COOMBS, R.; SAVIOTTI, P.; WALSH, V. (Ed.), *Technological Change and Company Strategies*: Economic and sociological perspectives, London: Academic Press, 1992. p. 132/161), apresentando uma solução para a vinculação do social e do econômico. Isto é, ele reúne dispositivos econômicos sobre a circulação de mediadores, tais como ativos, contratos etc. e noções sociológicas sobre como os atores são definidos através de suas relações na conformação de redes (o que aqui não será tratado).

[57] Como o tem entendido Martín Carranza Torres, isto é, "[...] uma tendência cultural para a geração de conhecimento e seu aproveitamento integral por parte da comunidade na qual esses conhecimentos são produzidos" (*El Derecho de la Innovación Tecnológica*. Una historia del tecnotropismo capitalista. Buenos Aires, 2008. p. 4).

conhecimento, necessitando intervir para assegurar a sua segurança, acarretando uma ampliação dos mecanismos de vigilância em detrimento de direitos humanos e fundamentais muito caros aos indivíduos, mas também de alta relevância para a ordem social como um todo. Assim, as tecnologias de vigilância e sua aplicação pelos Estados-nação são permanentes ameaças à democracia, à liberdade de expressão e à privacidade. Com o escopo de restabelecer o controle sistemático em tal seara, o que é apropriado em nações democráticas, não poderá o Estado, contudo, gerar situações de violação de direitos mais graves do que as que foram cometidas eventualmente para salvaguardar a privacidade, a dignidade e os liberdades fundamentais. De todo modo, segue sem resposta a seguinte pergunta: *Quem está vigiando os vigilantes*?