XXIV CONGRESSO NACIONAL DO CONPEDI - UFMG/FUMEC/DOM HELDER CÂMARA

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS

JOSÉ RENATO GAZIERO CELLA

AIRES JOSE ROVER

MAGNO FEDERICI GOMES

Copyright © 2015 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Todos os direitos reservados e protegidos.
Nenhuma parte deste livro poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria – Conpedi
Presidente - Prof. Dr. Raymundo Juliano Feitosa – UFRN
Vice-presidente Sul - Prof. Dr. José Alcebíades de Oliveira Junior - UFRGS
Vice-presidente Sudeste - Prof. Dr. João Marcelo de Lima Assafim - UCAM
Vice-presidente Nordeste - Profa. Dra. Gina Vidal Marcílio Pompeu - UNIFOR
Vice-presidente Norte/Centro - Profa. Dra. Julia Maurmann Ximenes - IDP
Secretário Executivo -Prof. Dr. Orides Mezzaroba - UFSC
Secretário Adjunto - Prof. Dr. Felipe Chiarello de Souza Pinto – Mackenzie

Conselho Fiscal
Prof. Dr. José Querino Tavares Neto - UFG /PUC PR
Prof. Dr. Roberto Correia da Silva Gomes Caldas - PUC SP
Profa. Dra. Samyra Haydêe Dal Farra Naspolini Sanches - UNINOVE
Prof. Dr. Lucas Gonçalves da Silva - UFS (suplente)
Prof. Dr. Paulo Roberto Lyrio Pimenta - UFBA (suplente)

Representante Discente - Mestrando Caio Augusto Souza Lara - UFMG (titular)

Secretarias
Diretor de Informática - Prof. Dr. Aires José Rover – UFSC
Diretor de Relações com a Graduação - Prof. Dr. Alexandre Walmott Borgs – UFU
Diretor de Relações Internacionais - Prof. Dr. Antonio Carlos Diniz Murta - FUMEC
Diretora de Apoio Institucional - Profa. Dra. Clerilei Aparecida Bier - UDESC
Diretor de Educação Jurídica - Prof. Dr. Eid Badr - UEA / ESBAM / OAB-AM
Diretoras de Eventos - Profa. Dra. Valesca Raizer Borges Moschen – UFES e Profa. Dra. Viviane Coêlho de Séllos Knoerr - UNICURITIBA
Diretor de Apoio Interinstitucional - Prof. Dr. Vladmir Oliveira da Silveira – UNINOVE

D598

Direito, governança e novas tecnologias [Recurso eletrônico on-line] organização CONPEDI/ UFMG/FUMEC/Dom Helder Câmara;
coordenadores: José Renato Gaziero Cella, Aires Jose Rover, Magno Federici Gomes – Florianópolis: CONPEDI, 2015.

Inclui bibliografia
ISBN: 978-85-5505-123-4
Modo de acesso: www.conpedi.org.br em publicações
Tema: DIREITO E POLÍTICA: da vulnerabilidade à sustentabilidade

1. Direito – Estudo e ensino (Pós-graduação) – Brasil – Encontros. 2. Governança. 3. Novas tecnologias. I. Congresso Nacional do CONPEDI - UFMG/FUMEC/Dom Helder Câmara (25. : 2015 : Belo Horizonte, MG).

CDU: 34

CONPEDI
Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Florianópolis – Santa Catarina – SC
www.conpedi.org.br

XXIV CONGRESSO NACIONAL DO CONPEDI - UFMG/FUMEC /DOM HELDER CÂMARA

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS

Apresentação

PREFÁCIO

O XXIV Congresso Nacional do CONPEDI, realizado em Belo Horizonte, nos dias 11 a 14 de novembro de 2015, foi promovido pelo CONPEDI, pela Universidade Federal de Minas Gerais (UFMG), pela Fundação Mineira de Educação e Cultura (Universidade FUMEC) e pela Escola Superior Dom Helder Câmara, tendo como tema geral o Direito e política: da vulnerabilidade à sustentabilidade.

O grupo de trabalho Direito, Governança e Novas Tecnologias foi bastante exitoso, tanto pela ótima qualidade dos artigos apresentados, quanto pelos debates entre os pesquisadores-expositores, interessados e coordenadores. Foram apresentados 26 trabalhos, efetivamente discutidos e que integram esta obra, a partir de 04 blocos temáticos: o primeiro, a democracia e a tecnologia; o segundo, a proteção de dados; o terceiro, a governança eletrônica; e o quarto, os direitos fundamentais e sociais na sociedade informacional.

As relações entre a democracia e as novas tecnologias comprovaram a complexidade do tema e foram representadas pelos seguintes trabalhos: a ampliação dos canais de comunicação entre as universidades publicas federais e a sociedade: os portais institucionais como mecanismos para implementar um novo modelo de governança, que analisou a transparência e o sigilo a partir da Lei de Acesso à Informação. A cidadania virtual e os obstáculos a sua efetivação, que estudou a ampliação de acesso à internet como instrumento de luta contra a globalização hegemônica. A internet como espaço público para participação politica no Estado Democrático de Direito: uma ágora digital?, que pesquisou os novos conceitos de cidadania e cultura digitais, fomentando atos ativistas para controlar excessos. Acesso à informação pública: a sociedade civil descobrindo o estado, que trabalhou a emancipação social por meio de políticas públicas de acesso à informação como modo de implementar a cidadania. Internet: uma nova forma de participação democrática ou um mero espaço de fiscalização digital? demonstrou a baixa confiabilidade da população na informação fornecida pelas mídias eletrônicas, especialmente pela linguagem inacessível a grande parte da sociedade. Por sua vez, o uso de instrumentos tecnológicos no exercício da democracia através da participação nas políticas públicas trouxe proposta de utilização de instrumentos tecnológicos para ampliar o espaço democrático e qualificar os serviços públicos.

Finalmente, o artigo redes sociais e democracia deliberativa comentou a ação política performática e a impossibilidade de enfrentamento racional no debate político na rede.

No que toca à proteção de dados e a necessidade de sua tutela diferenciada, o texto o `curtir´ do facebook como manifestação da liberdade de expressão: uma nova tecnologia sob proteção constitucional estudou a análise do perfil ideológico dos trabalhadores por empregadoras como forma de justificar dispensas. O trabalho a vida escrita em bytes - a sociedade superinformacional e as novas tecnologias: será o fim da privacidade e da dignidade humana? analisou as consequências jurídicas e emocionais da exposição das informações privadas na rede, o que viola a dignidade da pessoa humana e gera a vulnerabilidade do indivíduo. Com isso, o artigo autodeterminação informativa e proteção de dados: uma analise critica da jurisprudência brasileira estudou a aceitação de sistemas de pontuação dos consumidores pelos Tribunais pátrios, a partir de conceitos distintos: banco de dados / dados estatísticos. Direito ao esquecimento digital e responsabilidade civil dos provedores de busca na internet: interface entre marco civil, experiência nacional e estrangeira e projetos de lei nº 7881/2014 e nº 1676/2015 tratou do direito ao esquecimento como consectário do direito a privacidade. Os novos cadastros e bancos de dados na era digital: breves considerações acerca de sua formação e do atual tratamento jurídico demonstrou o viés econômico das informações constantes na internet e trouxe o fenômeno da necessidade de autoafirmação das pessoas oposta ao sentimento de privacidade. Por fim, a pesquisa a usurpação do registro civil nacional pelo Poder Judiciário comentou a necessidade do asseguramento de dados sensíveis e a retirada da atribuição de guarda de tais informações do Executivo e o texto riscos inerentes a utilização de redes informáticas, com foco no risco a privacidade e a segurança cibernética trouxe a incompatibilidade entre segurança e privacidade e as inovações tecnológicas mais atuais.

A partir de tais discussões, adentrou-se na temática governança eletrônica e seus escopos no Direito informático. O estudo a utilização das TIC e a contribuição das cidades digitais para o favorecimento da governança concluiu que a criação das cidades digitais facilitou o acesso ao serviço público e ao `e-commerce´, mas não trouxe avanços em matéria de governança, apesar de possuir potencial para isso. A analise crítica da legitimidade do Estado a partir da aplicação do princípio da resiliência demonstrou como o Estado pode manter sua estrutura e abrir novos canais de comunicação e participação da sociedade civil para a tomada de decisões, por meio dos princípios da resiliência, consensualidade, cooperação e concertação nos atos administrativos. No seu tempo, o texto "governança da internet no espaço regulatório global: o idiossincrático modelo de gestão da ICANN" tratou da necessidade de regulação da internet, pelo ICANN ou pelos Estados Unidos da América, dentro da concepção do `policy making´.

Entre as pesquisas dedicadas aos direitos fundamentais e sociais na sociedade informacional, o artigo a internet como vetor do desenvolvimento social na contemporaneidade encampou a ideia de desenvolvimento como liberdade e as ondas de acesso à internet. "As novas tecnologias em prol do trabalhador: tentativas de minimizar o retrocesso aos direitos sociais" ofereceu um panorama da inserção do trabalhador nas novas tecnologias e como deveria ser visto o teletrabalho, caso houvesse um efetivo controle de ponto via `smartphones´, cujo problema também foi tratado pelo texto "teletrabalho e tecnologia: (re) adaptações sociais para o exercício do labor", que apresentou o conceito inovador de subordinação por meio de sistemas telemáticos e a ruptura do paradigma no Direito laboral. "Imigrantes no Brasil - discursos de ódio e xenofobia na sociedade da informação: como atribuir uma função social a internet?" elucidou o contraponto entre a sociedade da informação e a função social da rede e como os processos simbólicos sobrepõem o objeto à pessoa, o que comprovou que a internet encontra-se à margem do Direito nas tratativas dos discursos de ódio. A economia compartilhada e os desafios na atuação do Estado foram os temas de "sociedade civil, concentração econômica e a disrupção da economia compartilhada", que relacionou os valores caros à democracia, entre eles os direitos fundamentais, e a dificuldade de regulação estatal. Em sequência, a "análise dos principais projetos municipais de acesso livre e gratuito a internet em praças publicas: inclusão digital na atual sociedade da informação globalizada" sugeriu, por meioi de pesquisa empírica, que as praças públicas deveriam ser implementadas nas periferias, em primeiro lugar, para promover a inclusão digital. Ao seu turno, o trabalho "as tecnologias da informação e comunicação no aprimoramento do processo legislativo: fundamentos para um processo legislativo mais interativo" partiu do pressuposto de que a democracia representativa brasileira é inacabada, para indicar a necessidade de ampliação da participação social na função legiferante. O artigo "grupos de fato na sociedade da informática" trata sobre as redes de informação e sua influência na transmissão dos conhecimentos tradicionais entre e para os povos formadores da sociedade brasileira. Finalmente, "o tempo morto de trabalho no processo eletrônico" demonstrou, por meio de análise de dados empíricos, que os processos eletrônicos não vieram a implementar a razoável duração dos procedimentos e geraram óbice ao `jus postulandi´ na Justiça Especializada do Trabalho, diminuindo o acesso à jurisdição.

Como conclusão, a coordenação sintetizou os trabalhos do grupo e sugeriu novos estudos a partir da leitura atenta dos artigos aqui apresentados e da cooperação entre os Programas de Pós-graduação, o que contribuirá para que novas respostas possam ser apresentadas para os dilemas que se multiplicam nesta sociedade informacional.

Os artigos, neste momento publicados, objetivam fomentar a investigação interdisciplinar entre o Direito, a Governança e as Novas Tecnologias. Assim, convida-se o leitor a uma leitura analítica desta obra.

Os Coordenadores

José Renato Gaziero Cella

Magno Federici Gomes

Aires José Rover

RISCOS INERENTES A UTILIZAÇÃO DE REDES INFORMÁTICAS, COM FOCO NO RISCO À PRIVACIDADE E A SEGURANÇA CIBERNÉTICA

INHERENT RISKS OF THE USE COMPUTER NETWORKS, WITH FOCUS ON RISK TO PRIVACY AND CYBER SECURITY

Ronaldo Bach da Graça

Resumo

O presente trabalho aborda aspectos da internet como meio de comunicação de massa e outros riscos contextualizados no tema, aspectos da realidade nacional no que concerne a segurança cibernética, políticas públicas e normas utilizadas para a implementação da Segurança Cibernética no Brasil. O trabalho tem por objetivo auxiliar a sociedade a decidir de forma consciente se vale a pena a implementação da segurança cibernética e qual seria o limite em contraponto a mitigação da privacidade, de forma a realizar uma vigilância adequada dos sistemas virtuais. O texto segue o método de abordagem descritivo e lógico-intuitivo, abordando riscos inerentes a utilização de redes informáticas, com foco no risco à privacidade e a segurança cibernética.

Palavras-chave: Riscos, Redes informáticas, Privacidade, Segurança cibernética

Abstract/Resumen/Résumé

This work approaches aspects about the internet as a way of mass communication and other risks related to the internet, aspects about the national situation related to the cyber security, public policies and rules used to the implementation of the cyber security in Brazil. This work aims to help the society to decide consciously if it is worth the implementation of the cyber security and what the limit is -, despite the mitigation of the privacy, in order to provide an adequate surveillance of the virtual systems. The research was made by the method of descriptive and logical-intuitive approach, exploring inherent risks of the use computer networks, with focus on risk to privacy and cyber security.

Keywords/Palabras-claves/Mots-clés: Risks, Computer networks, Privacy, Cyber security

INTRODUÇÃO

Mitigar a própria privacidade em favor de uma maior segurança no contexto de vida em comunidade foi uma opção evidenciada em pesquisas junto à população estadunidense[1]. A medir pela quietude da sociedade brasileira sobre o tema, ou se pensa de forma similar, ou se ignoram os riscos envolvidos.

O presente estudo pretende fomentar o necessário debate social sobre a influência da implementação da segurança cibernética na privacidade pela compreensão do que se entende por segurança cibernética, por uma análise da internet como meio de interação de massa e uma síntese suficiente para fomentar o debate que aborde os riscos já assumidos na internet que englobem vida privada; contextualizados na realidade brasileira.

O professor Ayres Britto (2012, p. 77-79) leciona que o sentimento *catapulta* para o mundo dos valores, qualificando a existência, aninhados nas regiões ônticas do civismo, da ética, da verdade – fomentando a justa decisão para o caso concreto. Esta pesquisa contribui para que a aludida *catapulta* seja veículo de decisões conscientes e justas, focando numa comunidade com maior qualidade de vida.

Por meio do fomento ao debate sobre um tema atual, todavia explorado, por vezes, com superficialidade, pretende-se potencializar a segurança jurídica de quem se vê envolvido como parte na discussão: queira-se ou não, toda a sociedade, mas em especial os profissionais de segurança cibernética, para que saibam com clareza quais os limites escolhidos pela sociedade para a sua atuação. Previne-se, desta forma que hajam de forma diferente do que espera a sociedade. É natural que tais profissionais evitem polêmicas jurídicas no exercício de sua profissão, motivo pelo qual quanto mais é sabido o limite da atuação destes que trabalham para proteger a sociedade, melhor será o resultado de seu labor, dentro do que deles se espera.

Nos dizeres de Marcio Iório Aranha (2014, p. 2), quando se preza pela segurança, fornece-se base sustentadora para identificação de juridicidade sem sujeitar sua modificação a critérios aleatórios. E o debate queda por fomentar segurança jurídica. Se os profissionais agirem aquém da necessidade para que se forneça um mínimo de segurança cibernética, que seja por decisão da sociedade que sofrerá as consequências de sua decisão anterior.

Para um fomento proveitoso, espera-se abordar: o que é segurança cibernética? Por que segurança cibernética seria importante para a sociedade brasileira? O quão a segurança cibernética mitigará a privacidade das pessoas mais do que já está mitigada em razão de usos

[1] Pesquisa citada no programa Debate, exibido pela Globo News em 11/06/2013.

de redes informáticas? É boa a relação custo/benefício para se investir em segurança cibernética?

O tópico 1 aborda aspectos da internet como meio de interação de massa; o tópico 2 trata do e-mail do Google; o tópico 3, enfoca sobre riscos; o tópico 4, discorre sobre políticas públicas e normas utilizadas para a implementação da Segurança Cibernética no Brasil.

O trabalho pretende oferecer meios para que a sociedade decida de forma consciente até que ponto vale a pena a implementação da segurança cibernética em contraponto a mitigação da privacidade, necessária para uma vigilancia adequada dos sistemas virtuais.

1. A INTERNET COMO MEIO DE INTERAÇÃO DE MASSA

Atualmente, as redes de computadores fazem parte da vida das pessoas: são utilizadas para interagir com pessoas queridas, obter informações, trabalhar, aprender, verificar resultados de exames médicos, para a segurança das casas, para monitorar animais domésticos, idosos, crianças, marcar consultas, demandar por bens e serviços, rastrear objetos em trânsito, facilitar processos logísticos, enviar livros para editora, enviar matérias jornalísticas (que podem ser impressas e/ou publicadas na própria rede mundial de computadores), ouvir ou baixar músicas, filmes, softwares, verificar o melhor caminho a se seguir, motorizado ou a pé, e até mesmo para enviar e-mails. As preferências pessoais dos que tem acesso à rede estão, em regra, a um clique de distância.

Mesmo os que não são chegados em tecnologias de computadores, estão obrigados a demandar por seus préstimos: até para cumprir com obrigações impostas pelo Estado, deve-se utilizar a rede mundial de computadores, e nela trafegar dados privados como aqueles declarados para a Receita Federal na oportunidade em que se declara o imposto de renda.
Trata-se de dados pessoais transitando na rede em razão de uma determinação normativa.

E-mails são trocados, por vezes, como único meio de comunicação disponível com determinado interlocutor. Diga-se de passagem, ainda que uma pessoa envie *e-mails* esporadicamente, pode eventualmente recebe-los em grande quantidade.

E todos os dados que trafegam pela rede permitem análise em determinado contexto. Ou em outras palavras, implicam em risco à privacidade: quando se consulta uma rota de deslocamento, pode-se presumir o interesse no caminho; quando se pesquisa o preço de uma passagem, pode-se presumir o interesse pela compra, quando se compram livros jurídicos, pode-se presumir que provavelmente se trata de um operador do Direito ou de alguém que deseja analisar juridicamente determinado caso concreto – e neste caso a compra será

eventual. E-mails recebidos, por vezes, podem ser relacionados com hábitos de consumo. Não é necessário o *envio* do *e-mail* para possibilitar análise, bastando o recebimento.

Quando se lê ou envia conteúdos de qualquer espécie, pode-se concluir por preferências pessoais. Quando se realiza um protesto contra políticos da situação no *Facebook* ou outra rede social, pode-se expor pessoalmente: na hipótese de o referido protesto ter sido feito por um detentor de cargo em comissão no governo, corre, o profissional, grande risco de perder o cargo confiado. Ou pior: quem não defende publicamente o chefe pode ter represálias no trabalho a depender da função que desempenhe.

Quando se transita um resultado de exame de saúde na rede, pode haver interceptação das informações, e terceiros terem acesso a eventual risco de saúde *pessoal*. Nas hipóteses de interação bancária, além do risco de ter sua comunicação interceptada e/ou divulgada, ainda se corre o risco de trafegar na rede dados suficientes para que seja implementado um furto em determinada conta bancária.

Ao se baixar filmes, demonstra-se a preferência do usuário, por vezes preferências íntimas. Ao se acessar o site de uma clínica veterinária, demonstra-se o vínculo da pessoa com animais.

Mesmo quem não quer se sujeitar a exposição na rede mundial de computadores, algumas vezes não possui outra opção: vai se expor, como na hipótese em que seus dados pessoais trafegam com destino à Receita Federal ou a determinados serviços que só funcionam pela internet como o seguro de viagem para a maior parte dos usuários de cartão de crédito *premium*.

Toda oferta de dados por parte do usuário/consumidor implica em riscos. O simples acesso a uma rede é fonte de dados potencial para curiosos. Muitas vezes estes dados trafegam em claro na internet: é como se a vítima potencial da captura de dados falasse assuntos privados numa intensidade suficiente para que terceiros tivessem acesso. Mas fugir deste tipo de risco tem sido difícil: atualmente uma pessoa sem endereço eletrônico teria dificuldade de ser considerada não excluída. Além do que, basta a conexão para maximixar a ameaça. Nesta hipótese, a troca de dados entre meios informáticos pode até ser considerado como um fator a mais de risco.

O endereço eletrônico pode ser considerado hoje o endereço virtual da maior parte das pessoas que acessa a internet. A “casa virtual” da maior parte das pessoas. Mas deve-se entender como funciona a vida privada na Internet para que se possa ao menos ter uma opinião que contribua com a comunidade.

São poucas as hipóteses de um empreendimento privado agir sem intuito de lucro. Quem acessa a internet pode perceber que existem muitos serviços “gratuitos” para o usuário, mas que nem por isso deixam de visar ao lucro: não existe almoço de graça.

2. O CASO DO GMAIL

O serviço de e-mail gratuito é um bom exemplo: deve-se meditar acerca do que leva um empreendimento que visa ao lucro, num contexto de sociedade capitalista, oferecer e-mail gratuito para alguém. Pode-se ter a certeza de que alguém paga a conta. E o questionamento que fica seria de com que motivação.

Percebe-se que o usuário do e-mail não paga pelo serviço porque o produto é ele próprio – o usuário. Dados do usuário podem ser altamente cobiçados por patrocinadores. Exemplifique-se por meio de um dos mais populares e-mails gratuitos da internet, o Gmail.

Segundo o portal de negócios Exame, a empresa Google teria se manifestado no sentido de que seus usuários de e-mail gratuito não devem ter expectativa por privacidade: as mensagens não são restritas a expedidor e destinatário. Segundo o Google, as mensagens são processadas pelo provedor. Um pouco mais que isso: em razão da norma estadunidense conhecida por *Patriot Act*, é possível ainda que as informações processadas sejam disponibilizadas às autoridades americanas (RUIC, 2015).

Ao cruzar dados fornecidos voluntariamente pelos usuários nos mais diversos serviços disponibilizados pelo Google, pode-se agregar uma maior eficiência, nos anúncios vendidos pela empresa. Com a publicidade mais bem direcionada, pode-se cobrar mais caro aos anunciantes, maximizando o lucro (PORTAL VEJA, 2015). Em outras palavras: não existe e-mail de graça. Pode ser que saia mais barato pagar pelo serviço.

Corroborando com a constatação, a *Consumer Watchdog* informou que as mensagens postadas nos servidores do Google podem ser acessados por uma “infinidade de motivos”, sendo o mais comum a venda de anúncio para clientes. Os procuradores do Google se manifestaram no sentido de que *uma pessoa não pode ter expectativas legítimas de privacidade na informação que envia voluntariamente a terceiros*, indicando claramente a possibilidade de acesso por outras pessoas das mensagens de *e-mail*. Note-se que as mensagens, nesta hipótese, não mais são pessoais, e os usuários concordam com a hipótese ao aceitarem os termos do serviço. Ao defender a empresa seus procuradores ainda manifestaram que *estão tentando criminalizar práticas comerciais normais*. A varredura de dados é prevista nos Termos de Uso e Política de Privacidade dos serviços da empresa (PORTAL TECNOMUNDO, 2015).

O Google, ao explanar sobre sua política de privacidade, expõe que coletam:

(...) informações para fornecer serviços melhores a todos os nossos usuários, desde descobrir coisas básicas, como o idioma que eles falam, até coisas mais complexas, como **anúncios que o usuário pode considerar mais úteis**, **as pessoas on-line que são mais importantes para o usuário** ou os vídeos do YouTube dos quais o usuário poderá gostar.

Coletamos informações de duas maneiras:

- **Informações fornecidas pelo usuário.** Por exemplo, muitos de nossos serviços exigem a inscrição em uma Conta do Google. Quando o usuário abre essa conta, pedimos informações pessoais, como nome, endereço de e-mail, número de telefone ou **cartão de crédito**. Se o usuário quiser aproveitar ao máximo os recursos de compartilhamento que oferecemos, podemos também pedir-lhe para criar um Perfil do Google publicamente visível, que pode incluir nome e foto.
- **Informações que coletamos a partir do uso que o usuário faz dos nossos serviços. Coletamos informações** sobre os serviços que o usuário utiliza e como os usa, por exemplo, quando assiste a um vídeo no YouTube, visita um website que usa nossos serviços de publicidade ou quando **vê e interage com nossos anúncios** e nosso conteúdo. Essas informações incluem:
  - **Informações do dispositivo**

Coletamos **informações específicas de dispositivos** (por exemplo, modelo de hardware, versão do sistema operacional, identificadores exclusivos de produtos e informações de rede móvel, inclusive número de telefone). A Google pode associar **identificadores de dispositivo** ou **número de telefone** à Conta do Google do usuário.

  - **Informações de registro**

Quando o usuário utiliza nossos serviços ou vê conteúdo fornecido pela Google, nós coletamos e armazenamos automaticamente algumas informações em registros do servidor. Isso inclui:

- detalhes de como o usuário utilizou nosso serviço, como suas consultas de pesquisa.
- informações de registro de telefonia, como o número de seu telefone, número de quem chama, números de encaminhamentos, horário e data de chamadas, duração das chamadas, informações de identificador de SMS e tipos de chamadas.
- Endereço de protocolo de Internet (IP)
- informações de evento de dispositivo como problemas, atividade de sistema, configurações de hardware, tipo de navegador, idioma do navegador, data e horário de sua solicitação e URL de referência.
- cookies que podem identificar exclusivamente seu navegador ou sua Conta do Google.

  - **Informações do local**

Quando o usuário utiliza os serviços da Google, podemos **coletar e processar informações sobre a localização real dele**. Além disso, usamos várias tecnologias para determinar a localização, como endereço IP, GPS **e outros sensores** que podem, por exemplo, fornecer à Google informações sobre dispositivos, **pontos de acesso Wi-Fi e torres de celular próximos**.

  - **Números de aplicativo exclusivos**

Determinados serviços incluem um número de aplicativo exclusivo. Este número e as informações sobre sua instalação (por exemplo, o tipo de sistema operacional e o número da versão do aplicativo) devem ser enviados à Google quando o usuário instalar ou desinstalar esse serviço ou quando esse serviço entrar em contato periodicamente com nosso servidores, como para atualizações automáticas.

  - **Armazenamento local**

Podemos coletar e armazenar informações (inclusive informações pessoais) localmente em seu dispositivo usando mecanismos como armazenamento no navegador da web (inclusive HTML 5) e caches de dados de aplicativo.

  - **Cookies e identificadores anônimos**

> Nós **e nossos parceiros** usamos várias tecnologias para coletar e armazenar informações quando o usuário visita um serviço da Google.Tais informações podem incluir o envio de um ou mais cookies ou identificadores anônimos para o dispositivo do usuário. Também usamos cookies e identificadores anônimos quando o usuário interage com serviços que oferecemos a nossos parceiros, como **serviços de publicidade** ou recursos da Google que podem aparecer em outros sites. Nosso produto Google Analytics ajuda empresas e proprietários de sites a analisar o tráfego nos respectivos websites e apps. Quando as informações do Google Analytics são usadas com nossos serviços de publicidade, como os que usam o cookie DoubleClick, elas são **vinculadas, por meio da tecnologia da Google, a informações sobre visitas a diversos sites** (GOOGLE, 2015).

Em síntese, a empresa coleta informações pessoais fornecidas pelo usuário, informações pessoais decorrentes de análise do perfil do usuário baseado em toda interação existente em seus servidores, inclusive sobre anúncios os quais o usuário aceita pedir por mais informações (eventualmente clicando num anúncio). A empresa identifica os dispositivos utilizados para acessar os sites da Google, informações sobre a rede móvel, inclusive número de telefone (se for o caso), número de quem chama e com que frequência, pontos de *wi-fi*, geolocalização por GPS (sistema de posicionamento global) - quando disponível, endereço eletrônico da máquina utilizada para acessar os serviços (difere do *e-mail*), informações (inclusive pessoais) localizadas no dispositivo pessoal, as quais o site tem acesso. Chega-se ao requinte de saber a versão de dispositivos instalados.

Pode-se perceber que as informações coletadas podem compor o sonho de um cônjuge, amante ou namorado ciumento. São informações extremamente íntimas, quiçá comprometedoras. Talvez a mãe de um filho adolescente saiba menos a respeito de seu filho do que o Google (potencialmente), caso este filho acesse aos serviços disponibilizados pela empresa com alguma frequência.

E a empresa informa sobre o que acontece com os dados coletados a partir da exposição voluntária do usuário:

> Como usamos as informações que coletamos:
> Usamos as informações que coletamos em todos nossos serviços para fornecer, manter, proteger e melhorar esses serviços, desenvolver novos e proteger a Google e nossos usuários. Também usamos essas informações para oferecer ao usuário um conteúdo específico - como fornecer para o usuário resultados mais relevantes de pesquisa e anúncios.
> Podemos usar o nome que o usuário fornece em seu Perfil do Google em todos os serviços que oferecemos e que exijam uma Conta do Google. Além disso, podemos substituir seus nomes antigos associados com sua Conta do Google de modo que o usuário esteja representado de maneira consistente em todos nossos serviços. Se outras pessoas já tiverem o e-mail ou outras informações que identifiquem o usuário, nós podemos mostrar-lhes estas informações do Perfil do Google que são publicamente visíveis (como nome e foto).
> Se o usuário tem uma Conta do Google, o nome e a foto do perfil, bem como as ações realizadas em aplicativos do Google ou de terceiros que estejam conectados a essa Conta do Google (como marcações +1, avaliações e comentários postados), podem aparecer nos nossos serviços, inclusive para exibição em anúncios e em

> outros contextos comerciais. Respeitamos as opções de compartilhamento limitado ou configurações de visibilidade que o usuário faz para a Conta do Google.
> Quando o usuário entra em contato com a Google, mantemos um registro da comunicação para ajudar a resolver qualquer problema que ele possa estar enfrentando. Podemos usar o endereço de e-mail do usuário para informar a ele sobre nossos serviços, por exemplo, as próximas mudanças ou melhorias.
> Usamos as informações coletadas de cookies e de outras tecnologias, como etiquetas de pixel, para melhorar a experiência do usuário e a qualidade geral dos nossos serviços. Um dos produtos que usamos para fazer isso com nossos próprios serviços é o Google Analytics. Por exemplo, quando o usuário salva suas preferências de idioma, nossos serviços aparecem no idioma que o usuário escolhe. Quando exibimos anúncios personalizados, não associamos cookies de navegador ou identificadores anônimos a categorias de questões sensíveis, como aquelas baseadas em raça, religião, orientação sexual ou saúde.
> Nossos sistemas automatizados analisam o conteúdo do usuário (incluindo e-mails) para fornecer recursos de produtos relevantes ao usuário, como, por exemplo, resultados de pesquisa e propaganda personalizados e detecção de spam e malware.
> Podemos combinar informações pessoais de um serviço com informações, inclusive informações pessoais, de outros serviços da Googlepara facilitar o compartilhamento de informações com pessoas que o usuário conhece, por exemplo. Não combinaremos informações do cookie da "DoubleClick" com informações de identificação pessoal, exceto se tivermos autorização do usuário (“opt-in”) para tanto.
> Solicitaremos sua autorização antes de usar informações para outros fins que não os definidos nesta Política de Privacidade.
> A Google processa informações pessoais em nossos servidores de muitos países do mundo. Podemos processar as informações pessoais do usuário em um servidor localizado fora do país em que este vive (GOOGLE, 2015).

O que na política é chamado de conteúdo específico pode ser traduzido como algo sobre o que provavelmente vai despertar o interesse do usuário, em razão do estudo prévio realizado a seu respeito. A empresa declara respeitar de forma “diferenciada” dados sobre em raça, religião, orientação sexual ou saúde. Informam ainda que os dados podem ser processados em um Estado diferente do de origem do usuário, portanto sujeito, eventualmente, a diferente norma legal do da origem dos dados, o referido processamento.

Perceba-se que se começou exemplificado a mitigação da privacidade em e-mails e as circunstância foram apontando para o fato de que está tudo integrado para fins de análise de usuário. Dados de *e-mails* são apenas mais um dado. Poderíamos falar de análise de dados de compras em cartão de crédito, mas se perderia o foco do trabalho.

Cônscio destas informações fica mais fácil descobrir como, *v.g.*, apareceu um SMS inesperado em seu *smartfone* (ou mesmo telefone mais simples) oferecendo determinado produto ou serviço que realmente é de seu interesse rotineiro. Ainda surpreende alguns o fato de que os anúncios disponibilizados na internet são mais interessantes do que os da televisão. São feitos sob medida para um usuário de perfil conhecido. Frise-se, mais uma vez, ser

conhecida ainda sua geolocalização, se for um feliz usuário de dispositivo informático com GPS ligado à rede mundial de Computadores[2].

Explanou-se sobre um único exemplo para que seja constatada mitigação da privacidade na rede por parte de uma das empresas nela presente. Deve-se, entretanto, ter em mente que empreendimentos privados, normalmente, estão investindo na rede com a finalidade de angariar lucros, pode-se visualizar que com outros exemplos o resultado não será muito diferente do que aqui foi tratado.

O lucro médio oferecido pelo usuário dos serviços gratuitos deve compensar o que a empresa investe para obter os dados a serem vendidos para terceiros. Anúncios muito direcionados e específicos costumam ter um custo relativamente elevado para o anunciante.

Da análise *supra*, decorre que: independente da norma legal de um Estado – qualquer que seja, o consumidor médio de internet já tem sua privacidade mitigada em todos os lugares do mundo, e dificilmente um legislador poderá reverter este quadro sem um consenso mundial sobre o regulação do tema, o que seria inédito. Eventual intervenção estatal seria mitigada pela jurisdição (territorialidade)[3].

A internet é um meio de comunicação de massa inovador, podendo ser chamado de meio de interação da massa. As pessoas podem interagir, e nesta interação elas se expõe, expondo sua privacidade, algumas vezes de forma consciente.

Difícil, no Brasil, achar um doutor que não possua sua vida profissional nas mãos de qualquer pessoa a poucos cliques de distância. Estudantes e pesquisadores queiram ou não, dependem de ferramentas de registro de currículo como a Plataforma Lattes[4], presente no país.

Se por meio desta única fonte de informações se pode descobrir muito de uma pessoa, imagine-se pela análise de grande parte do que faz na rede, com que equipamentos, com que frequência, com que contatos.

Para enumerar apenas riscos à privacidade, já se pode dizer de antemão que o rol será meramente exemplificativo. O Estado pode/deve proteger a sociedade dos riscos que a podem ameaçar. No caso do mundo virtual, tal proteção também depende de análise de riscos

---

[2] Informações armazenadas por meio de *cookies* contribuem com propagandas sobre medida. Outro exemplo pode ser constatado de posse de um iPhone (Versão 8.1.2 (12B440)), no caminho ajustes>privacidade>publicidade. Há uma opção que alguns não conhecem de "limitar publicidade rastreada".

[3] Para mais informações ler: ÁLVARES, João Gabriel. Territorialidade e Guerra Cibernética. In: Segurança e Defesa Cibernética: Da Fronteira Física aos Muros Virtuais. Org. Oscar Medeiros Filho et al. Recife: Ed. UFPE, 2014.

[4] Para saber mais, consulte: http://lattes.cnpq.br/

virtuais. A proteção virtual pressupõe vigilância, o que naturalmente mitiga a privacidade. Talvez menos do que ela já tem sido mitigada, talvez já com o conhecimento do usuário.

Percebe-se, pois que a privacidade é algo improvável na internet para um usuário comum, pois na rede mundial de computadores qualquer coisa é fonte de dados, o extrato do cartão de crédito eventualmente recebido por *e-mail* – frise-se ainda que dados privados podem circular na rede sem que a fonte dos dados sequer tome conhecimento. Estuda-se o potencial consumidor/usuário com o objetivo de que a ele sejam disponibilizados bens e serviços cativantes e do agrado da "vítima".

3. POTENCIALIZANDO O RISCO

Para Masi (2014, p. 529-616), novas tecnologias tem evidenciado a dicotomia entre analógicos e digitais, sendo os digitais aqueles que vivem de acordo com a cultura pós-moderna, e os analógicos estariam fadados à extinção. Afirma ainda, o autor, que os digitais convivem sempre com as novas tecnologias, apreciam conquistas científicas, conjugam relacionamentos virtuais com os reais. Por óbvio a internet é um dos símbolos desta geração pós-moderna. Por isso o autor ratifica que desde a sociedade pós-industrial a sociedade se preocupa com o controle normativo da tecnologia.

O controle normativo da internet é complicado de ser implementado, pelo fato de que redes informáticas não respeitam fronteiras físicas. Não se consegue facilmente impor uma normatização na rede; e pra que a sociedade tutele seus bens jurídicos de forma efetiva, deve investir em investigação preventiva e tecnologia.

De Masi (2014, p. 529-616) reconhece ainda que hodiernamente grande parte do trabalho pode ser – e tem sido - delegado às máquinas (e aos imigrantes). Tal constatação reforça a tese de que os trabalhos controlados por redes informáticas ganham cada vez mais espaço na sociedade, e demandarão cada vez mais segurança para que os fins sociais desejados sejam alcançados e mantidos.

Estados ricos podem defraudar impunemente os pobres, pois os pobres ainda são incapazes de deflagrar uma guerra mundial [com meios tradicionais de guerra], mesmo compondo dois terços da população mundial (MASI, 2014, p. 529-616). No entanto, quando se trata de guerra virtual ou ameaça eletrônica, talvez não seja tão impossível um ataque significativo deflagrado com poucos recursos financeiros, o que aumenta a necessidade de que seja preservada a segurança em redes informáticas.

Prestadores de serviços como bancos e lojas virtuais tendem a diminuir a necessidade de intermediários e aumentar a dependência social relacionada a redes informáticas (MASI,

2014, p. 529-616). Este conjunto de fatores já seria suficiente para convencer muitos que se deve assegurar o bom funcionamento de redes de computadores, e se deve tutelar, também no mundo virtual, os bens especialmente estimados pela sociedade.

A tutela a ser ofertada pelo Estado para a população passa pela regulação de uma tal guerra, quase nunca declarada, que acontece a todo tempo: tempo de paz, de crise e de guerra. Para que a tutela seja efetiva ela depende de regulação. E aqui se pode abrir um parêntese para lembrar o leitor que regulação difere de regulamentação. A regulamentação possui um viés político, enquanto a regulação é realizada por técnicos, que interpretam e implementam as políticas públicas desenhadas pela classe política por meio das leis. Os reguladores, com sua experiência e visão prospectiva de especialistas, expedirão atos técnicos e deles decorrerão decisões finalísticas quase legislativas (normativas) e quase judicantes que cumpram o que a sociedade vier a decidir pelo debate social, deforma a que as políticas públicas regulamentadas sejam implementadas.

Hoje se encontra presente uma fabulosa expansão informática; concomitantemente a mundialização de redes de comunicação instantânea dinamiza o mercado mundial e é dinamizada por ele. Toda essa inovação precisa de um ambiente favorável para que materialize o bem comum. Este ambiente favorável necessariamente passa por uma regulação difícil de implementar sem a aceitação de todos os Estados. Trata-se da emergência de infraestrutura, no caso jurídica, da sociedade-mundo a que Morin (2011, p. 17-93) se refere. Constata, o autor, que a sociedade mundial carece de leis, direito, controles; ratificando que as atuais instituições não estão aptas para efetuar tais regulações.

O que fazer com o *underground* planetário a que se refere Morin (2011) que se pode dizer que se replica na realidade virtual do mundo, com sua criminalidade atroz - passa a ser um desafio para tal regulação.

Os ataques de 11 de setembro de 2001, nos Estados Unidos, estimularam a formação de uma polícia mundial sem, no entanto estimular suficientemente uma política mundial (MORIN, 2011, p. 17-93). Tal fato reforçaria a tese de que há demanda para a regulação e para o aparelhamento da sociedade a fim de sejam evitados crimes, inclusive virtuais, respeitadas as diferentes culturas e a democracia. Instrumentos de força em favor da sociedade não fazem sentido sem democracia reconhecida por todos.

Por outro lado, Friedman (2010, p. 54-55) lembra que os ataques terroristas de 11 de setembro de 2001 desviaram uma enorme quantidade de energia, dinheiro e atenção para a instalação de equipamentos de segurança em aeroportos, estações de trem, prédios federais. Apesar de o autor usar esta assertiva para criticar o exagero no investimento em segurança em

detrimento de investimentos em infraestrutura, admite a necessidade da reação a fim de reforçar a vigilância das fronteiras, aprimorando serviços de inteligência. Tudo sempre buscando um equilíbrio nas ações. Considerou que não adianta construir uma cerca alta em torno de uma infraestrutura decadente. A sociedade deve discernir sobre o que realmente importa e como agir, de forma pragmática, esperando racionalmente resultados, sem desperdício de energia.

Disto se aduz que o excesso de investimento em segurança pode ser prejudicial à comunidade, remetendo ao reconhecimento de que a segurança é um instituto que pode contribuir com a vida em sociedade desde que seja implementada com equilíbrio.

Um mundo de abundância favorece a liberdade e a democracia, em contraposição, *um mundo de escassez favorece sempre o autoritarismo, visto que alguém terá que administrar o racionamento* (ROMM *apud* FRIEDMAN, 2010, p. 75).

A tendência de governantes ao autoritarismo que se evidencia inclusive em democracias não consolidadas deve ser combatida para que o Estado sirva ao povo, evitando o conceito de o Estado ser utilizado para subjugar ou se servir do povo que o fez nascer. Evidencia-se, portanto, temerária a disponibilidade de dados pessoais para uso político. Redes informáticas podem favorecer ou não a democracia, a depender de como são utilizadas.

Não bastasse a ameaça do terror, o crescimento populacional se tornou tão grande e rápido que Michael V. Hayden, diretor da Agência Central de Inteligência (CIA) declarou que seus analistas acreditam que a explosão demográfica é mais preocupante que o terrorismo, e se as necessidades básicas desta população não forem atendidas, uma grande massa pode ser atraída para a violência e extremismo (FRIEDMAN, 2010, p. 90-91).

Naturalmente a violência de que fala o autor pode ser implementada por meio da violência virtual, do que decorre a necessidade de defesa do mundo virtual para que as regras também sejam nele cumpridas.

A inovação e competição proporcionadas pela internet tem possibilitado integração de trabalhadores e de seus trabalhos por meio das redes de meios informáticos, trazendo sinergia para os trabalhos e competição entre trabalhadores espalhados pelo mundo (FRIEDMAN, 2010, p. 92-93). Até mesmo a manutenção de empregos de qualidade depende em muito, nos dias de hoje, de segurança na rede de sistemas informáticos.

Como já se percebeu, os computadores e afins comandam uma infinidade de máquinas que contribuem com o bem estar social e o aumento de bons empregos e da qualidade de vida. Um exemplo tipicamente brasileiro de uso de equipamentos que demandam por segurança cibernética é o uso da urna eletrônica. Estes equipamentos podem

ser tomados como base da legitimidade do sistema representativo nacional. Não se devem admitir riscos atrelados a tais equipamentos. Melhor seria a boa, velha e auditável urna com votos de papel, ou – ao menos – a combinação dos dois.

Noticiou-se que os EUA podem endossar oficialmente tese de fraude eletrônica nas eleições brasileiras de 2014. O periódico estadunidense *The New York Times* denunciou que os EUA investigavam a possibilidade de o governo venezuelano de Chávez estar ligado num suposto golpe eletrônico em urnas, em vários países. No centro da polêmica estaria um empresa venezuelana chamada Smartmatic. A referida empresa prestou serviços no Brasil por ocasião das eleições presidenciais de 2014 (TOGNOLLI, 2015). Sem intenção de entrar na polêmica de se procedem ou não tais acusações, o que se pretende por meio desta observação é que seja dada a devida importância para a segurança dos meios informáticos ligados em rede. Neste exemplo a suposta falha ou limitação dos sistemas pode excluir a legitimidade da representatividade política de um Estado.

Existem riscos que podem ser considerados ainda maiores, pois por meio de redes informáticas se pode ameaçar a segurança física de toda a sociedade. Pode ser colocado como exemplo o ataque massivo sofrido pelo Irã com o vírus Stuxnet, que teria infectado sessenta por cento dos computadores daquele país, incluindo os da Usina nuclear de Bushehr. O vírus foi considerado capaz de penetrar em sistemas de comando de infraestruturas como centrais elétricas e nucleares, represas e indústrias químicas (LA VANGUARDIA, 2015).

Pode-se, pois, concluir que sempre existe o risco até mesmo de um acidente nuclear em razão do mau uso de redes informáticas, pois nos dias de hoje elas são instrumento de comando de infraestruturas críticas. Em razão desta constatação, princípios jurídicos de razoabilidade, proporcionalidade, defesa da paz, repúdio ao terrorismo, cooperação, devem ser ponderados em contraponto ao direito à privacidade.

A segurança cibernética também impõe riscos, pois a guerra cibernética necessita como já citado, de vigilância sobre o que potencialmente pode ser uma ameaça contra infraestruturas críticas: reais ou virtuais.

Desta forma, a sociedade deve, num amplo debate, decidir se é razoável entender que o risco de vulnerabilidade virtual a que todos se sujeitam em razão da realidade das redes informáticas é aceitável ou se se deve mitiga-lo com o custo de certa mitigação da privacidade. Se a sociedade decidir pela mitigação da privacidade, esta deve ser feita de forma controlada e responsável, preferencialmente livre de ingerências políticas para que sejam afastados os relevantes riscos de uso de informações pessoais por governos, mas sem

finalidade de defesa da sociedade, mas somente de parte dela, como por exemplo um partido político.

O risco pode ser gerido dentro de uma lógica de custo/benefício, em razão da opção social, necessariamente após amplo debate. A capacidade do Estado será proporcional ao investimento realizado na segurança, sendo que o Estado deve proteger a sociedade respeitando os limites a ele confiados pela comunidade.

Na hipótese de a sociedade decidir pela mitigação da privacidade, deve-se ainda considerar que a sociedade não deve assumir o risco de que tais informações sejam utilizadas com finalidade política. Tal uso seria, potencialmente, tão ou mais destrutivo que uma bomba feita com pólvora. No mundo contemporâneo, talvez seja mais apropriado decidir pelo nível de mitigação à privacidade, pois relativizar a privacidade pode não mais ser uma opção em face da realidade dos fatos.

Manuel Castells (2013, p. 117-182) abordou sobre a possibilidade de uso político de dados disponíveis na rede mundial de computadores. Ao longo de sua obra intitulada Redes de Indignação e Esperança, pode-se aduzir que para uma sociedade democrática é fundamental cuidar para que eventuais dados coletados nunca sejam utilizados com finalidade de controlar quem faz oposição. O autor discorre sobre a hipótese de desobediência civil como protesto, e por vezes uma reação violenta do Estado, mitigada em razão de que a violência estatal acabava por ampliar a simpatia dos cidadãos pelos movimentos reivindicatórios que pregavam a desobediência civil. O autor narra que em alguns momentos os cidadãos necessitaram da ajuda de hackers para mitigarem os riscos de protestos contra Estados, por vezes democráticos e desenvolvidos.

O bom uso das redes informáticas acaba por contribuir ainda com a disposição do art. 3º, II, da CR/88: garantir o desenvolvimento nacional. Agora se deve decidir até que ponto vale a pena protege-la e de quais ameaças.

4. SEGURANÇA CIBERNÉTICA - CONCEITOS NORMATIVOS E ASPECTOS DA REALIDADE NACIONAL

O Estado brasileiro já percebeu os riscos decorrentes do uso de redes informáticas, e já possui alguma norma e alguma doutrina, utilizadas para que seja implementada certa segurança cibernética. Terrorismo e espionagem são grandes alvos a serem combatidos pela sociedade por meio da Defesa Cibernética.

A doutrina militar brasileira de comando e controle considera a Guerra Cibernética uma operação de informação, e sobre ele discorre nos seguintes dizeres:

> A Guerra Cibernética corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper ou destruir capacidades de comando e controle do adversário. Compreende ações que envolvem as ferramentas de tecnologia da informação para desestabilizar os STIC² do oponente e defender os próprios STIC². Abrange, essencialmente, as Operações em Redes de Computadores. A oportunidade para o emprego dessas operações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à Tecnologia da Informação (BRASIL, 2006. P.44).

E complementa:

> A Operação em Redes de Computadores engloba o ataque a redes de computadores, a proteção contra ataques e a exploração dessas redes para fins de produção de conhecimento de Inteligência (BRASIL, 2006. P.44).

A referida doutrina ainda discorre sobre ataque, defesa e exploração de vulnerabilidades em redes de computadores.

Considerando o aumento das ameaças e tentativas de ataques cibernéticos, e com a finalidade de garantia de disponibilidade, integridade, confidencialidade e autenticidade da informação e comunicações no âmbito da Administração Pública Federal, foi instituída a Portaria N° 45, de 8 set 09 do GSI-PR, que em seu art. 2º define Segurança Cibernética no âmbito do Governo Federal brasileiro nos seguintes termos:

> Art. 2º Considera-se Segurança Cibernética a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus Ativos de Informação e suas Infraestruturas Críticas.
> § 1º São Ativos de Informação os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.
> § 2º São Infraestruturas Críticas as instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade.

A arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no espaço cibernético, seus ativos de informação e suas Infraestruturas críticas da informação é um conceito de Segurança Cibernética proposto por Canongia e Mandarino (2009. p. 27).

O Estado brasileiro é um dos mais vulneráveis a ataques cibernéticos. Esta assertiva foi constatada por meio de uma pesquisa promovida pelo Centro de Estudos Estratégicos e Internacionais (CSIS), em parceria com a McAfee, fabricante de antivírus para computadores. A pesquisa comparou a segurança cibernética em quatorze países, dentre os quais Estados Unidos, China, Grã-Bretanha, Índia e Rússia. Foram retratadas as percepções de profissionais que atuam nos setores financeiro, energético, de recursos naturais, telecomunicações, transportes, químico, alimentício e de serviços públicos. Neste contexto, saiu na mídia estadunidense, em 2009, que dois apagões que ocorreram no Brasil em 2005 e 2007 teriam sido causadas por *hackers* com finalidade de extorsão. Dias depois desta divulgação, dezoito

estados brasileiros ficaram sem energia, supostamente por ataques cibernéticos, que teriam desligado a usina de Itaipú. No mesmo ano, a Empresa de telefonia Telefônica, justificou graves problemas em seu serviço de banda larga em razão de ataques cibernéticos (PORTAL BBC, 2015).

Na percepção de 59% dos entrevistados, os autores destes ataques podem ser governos estrangeiros; e os Estados Unidos e a China foram apontados como as maiores ameaças neste sentido. Hamadoun Touré, chefe da agência de telecomunicações da ONU em 2010, por ocasião do Fórum Econômico Mundial de 2010, opinou sobre um tratado internacional sobre o assunto para impedir uma guerra cibernética (PORTAL BBC, 2015).

O documento de mais alto nível a tratar de política de defesa nacional é o Decreto nº 5.484, de 30 de junho de 2005. O referido Decreto considera em seu item 1.3 que *a segurança pode ser enfocada a partir do indivíduo, da sociedade e do estado, do que resultam definições com diferentes perspectivas.* Discorre ainda que

> especialistas convocados pela Organização das Nações Unidas (ONU) em Tashkent, no ano de 1990, definiram a segurança como "uma condição pela qual os Estados consideram que não existe perigo de uma agressão militar, pressões políticas ou coerção econômica, de maneira que podem dedicar-se livremente a seu próprio desenvolvimento e progresso" (BRASIL, 2005).

A Estratégia Nacional de Defesa, de 2008, materializa a preocupação do Estado brasileiro com o risco cibernético, por meio da citação do sistema de defesa cibernética em diversas oportunidades. Destarte resta demonstrado que cresce de importância no Governo Federal a segurança e a defesa cibernéticas.

A Norma Complementar 05 /Instrução Normativa 01 do DSIC/GSIPR, dispôs sobre a criação, nos órgãos e entidades da Administração Pública Federal, de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR, e a Diretriz n˚ 0014 do Ministério da Defesa, delegou ao Exército atribuições atinentes ao setor cibernético no âmbito das Forças Armadas brasileiras.

A Portaria n˚ 03, de 29 de junho de 2009, do Gabinete do Comandante do Exército, padroniza que o setor cibernético deve ser tratado, no nível estratégico, como Defesa Cibernética, independente da possibilidade de que se entenda haver terminologia mais adequada, motivo pelo qual utilizar-se-á no presente artigo segurança cibernética e defesa cibernética como sinônimos, mesmo que não o sejam de fato.

A Secretaria de Assuntos Estratégicos da Presidência da República tem demonstrado interesse sobre o tema, e desde 2013, por meio de reuniões interministeriais, vem elaborando proposta de políticas públicas para o Setor Cibernético, voltada à segurança e defesa do espaço cibernético nacional (SAE/PR, 2015).

Dentro da Agência Brasileira de Inteligência existe um órgão chamado Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações. Tal Centro foi criado com o escopo de salvaguardar o sigilo das transmissões oficiais. Promove desta forma, a obtenção de algoritmos de Estado e de equipamentos de proteção e de transmissão de informações (ABIN, 2008). Tais providências talvez sejam suficientes para assegurar as comunicações próprias, todavia não são medidas de proteção absoluta. Frise-se que dados criptografados continuam sujeitos à interceptação e análise.

Ainda compondo o contexto nacional da Segurança Cibernética, os reflexos dos ataques e ameaças terroristas recentes, como os ataques de Nova Iorque em 2001, os recentes ataques terroristas na França, radicais postando vídeos que disseminam o terror na rede, por vezes com ameaças a países centrais (EL PAÍS, 2015), (YÁRNOZ, 2015), (WAKEFIELD, 2015), (FRANCE PRESSE, 2015).

Segundo a Agência Brasileira de Inteligência (ABIN, 2015),

> (...)especialistas em Terrorismo Cibernético costumam apoiar-se na concepção de cenários possíveis, mediante avaliações feitas a partir da quantificação das (1) vulnerabilidades conhecidas e existentes nos sistemas informatizados, das (2) ameaças hipotéticas e reais que sobre eles incidem, e, finalmente, do (3) valor estratégico, político ou econômico das informações operadas nesses sistemas.
>
> Em sua concepção popular mais comum, o atacante de sistemas informatizados é um jovem adolescente que pratica um ataque individual. Para o estudo do Terrorismo Cibernético, entretanto, tal conceito vem sendo ampliado, uma vez que os efeitos pretendidos buscariam impactos de longo prazo nos planos psicológico, econômico ou da segurança da população. As ações de resposta, por sua vez, deverão ser coordenadas no âmbito governamental, sob complexo gerenciamento e legislação específica. Dessa forma, o terrorista cibernético deve ser entendido não como um indivíduo, mas um grupo, suficientemente coordenado, especializado inteligente e disciplinado, com expressivos recursos financeiros, materiais, e disponibilidade de conhecimento e tempo. Naturalmente, a proteção contra hackers individuais deve ser sempre considerada, mas mantém-se importante analisar e prevenir a ameaça maior representada por adversários detentores de significativo e organizado potencial destrutivo.

A ameaça à paz social é significativa, acenando, pois, por medidas contra este sistema organizado. Ameaçados estão: a paz social, a qualidade de vida, a economia. Some-se a tal ameaça espionagem com viés meramente econômico que pode minar relevantes postos de trabalho pelo mero trânsito de informações.

Terroristas, cada vez mais, tem feito uso de redes informáticas como forma de potencializar seus ataques. Existem hackers que agem por motivações religiosas ou políticas. Normalmente recrutados por extremistas, entendem o respeito humano, por vezes, de forma diversa das comunidades ocidentais, e normalmente possuem uma tolerância bem menor aos que possuem opiniões divergentes das suas. São os chamados de *hacktivistas*, e são peça importante no cenário do terrorismo cibernético, também conhecido por *ciberterrorismo*. Atacam equipamentos informáticos e por vezes focam consequências que provoquem perdas de toda ordem, inclusive ambientais, econômicas, humanas (RAPOSO, 2007, p.46).

Exércitos estão sendo treinados para o que tem sido considerado um novo Teatro de Operações, e neste ainda desconhecido espectro da guerra, os prejuízos podem tomar grandes proporções: uma notícia veiculada em 2013 narrou um grupo de hackers Sírios invadindo a conta no *Twitter* da agência de notícias Associated Press. Pela publicação de uma mensagem falsa sobre ataques à bomba na Casa Branca, US$ 136 bilhões desapareceram de Wall Street em apenas dois minutos (MATSURA, 2015). Eis um exemplo que pode acontecer em tempos de paz.

A Comissão de Ciência da Defesa dos EUA sinalizou que hackers chineses teriam tido acesso a projetos de mais de 20 armamentos, dentre eles alguns de alto valor estratégico como o sistema de mísseis *Patriot* e o helicóptero *Black Hawk* (MATSURA, 2015). No Brasil, Receita Federal e o IBGE já foram alvos ataques que levaram à indisponibilidade de serviços e alterações em seus websites (BRANQUINHO, 2015).

Outra evidência dos riscos advindos da internet tem sido materializados até mesmo em ofertas de *offset* realizadas em razão da demanda dos Estados por esta tecnologia: os países tem implementado em Acordos de Compensação programas que contemplem transferência de conhecimento e de tecnologia sobre cibersegurança. A demanda tem sido uma das prioridades de muitos Estados importadores, a ponto de a Conferencia de primavera de 2015 da *Global Offset and Countertrade Association (GOCA)* prever um painel que trata especificamente do tema (GOCA, 2015).

CONCLUSÃO

A segurança cibernética pode trazer potenciais benefícios para a sociedade, em especial para a sociedade brasileira, visto que o país é considerado por especialistas, relativamente vulnerável a ataques cibernéticos. O desenvolvimento econômico, naturalmente, tem estimulado certa dependência dos meios informáticos ligados em rede. Por

consequência, a proteção de redes como a internet acaba por resguardar interesses econômicos e os interesses sociais a eles ligados. Em outras palavras, se pode afirmar que a segurança cibernética contribui sinergicamente com a qualidade de vida em toda a sociedade, fomentando, inclusive, a segurança jurídica.

A privacidade percebe-se, já está mitigada para os usuários da internet, independente de localização geográfica ou classe social onde se pode enquadrar determinado usuário, a ponto de a Comissão Europeia aconselhar seus cidadãos a abandonarem o Facebook em razão de preocupação com privacidade mitigada por dados postados na internet. A Comissão Europeia alega outra conclusão que se pode aferir da leitura deste trabalho: a legislação local não tem como garantir a proteção dos dados vinculados a um serviço estrangeiro (no caso constatado estadunidense - existe uma norma europeia que proíbe o envio de dados de usuários para os Estados Unidos). Trata-se de mais um episódio meramente exemplificativo, o que pode ser constatado pelo fato de haver representação contra Apple, Facebook, Microsoft, Skype e Yahoo junto ao Tribunal Europeu de Justiça, em Luxemburgo por motivos semelhantes atinentes a falta de privacidade (INFOMONEY, 2015).

Por certo a sociedade deve debater se ofertar segurança cibernética mitigará a privacidade das pessoas mais do que já está mitigada pelo simples uso diário da rede – ou pela simples conexão sem acesso, considerando-se sempre o famoso no meio jurídico usuário médio; e – levando esta resposta em consideração – oferecer segurança jurídica aos profissionais que atuam nesta área. O importante é que trabalhem em proveito da sociedade dentro da política pública decidida de forma consciente e por meio de grande debate social, considerando todos os riscos envolvidos.

REFERÊNCIAS

ABIN. **CEPESP**. Brasília, atualizada pela ABIN, 2008. Disponível em: <HTTP:// www.abin.gov.br/modules/mastop_publish/?tac=Institucional#missão> Acesso em 07 de fevereiro de 2011.

_____. **Repercussões da Contenção da Ameaça do Terrorismo Internacional na Economia Brasileira.** Disponível em: <http://www.abin.gov.br/modules/mastop_publish/?tac=224>. Acesso em: 11/3/2015.

ÁLVARES, João Gabriel. **Territorialidade e Guerra Cibernética.** In: Segurança e Defesa Cibernética: Da Fronteira Física aos Muros Virtuais. Org. Oscar Medeiros Filho et al. Recife: Ed. UFPE, 2014.

ARANHA. Marcio Iorio. **Interpretação Constitucional e as Garantias Institucionais dos Direitos Fundamentais.** 3ª ed. rev. atual. – Coleford, UK: Laccademia Publishing, 2014.

BBC. **Brasil é um dos países mais vulneráveis a ataques cibernéticos, diz pesquisa.** Disponível em: <http://www.bbc.co.uk/portuguese/noticias/2010/02/100201_ataque_cibernetico_vdm.shtml>. Acesso em: 11/3/2015.

BRASIL. **Decreto nº 5.484, de 30 de junho de 2005.** Política de Defesa Nacional. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5484.htm>. Acesso em 20 nov. 2014.

_____. Ministério da Defesa. **MD31 – D – 03: Doutrina Militar de Comando e Controle.** Brasília, 2006.

BRANQUINHO, Marcelo Ayres . **A Cyberguerra bate em nossa porta.** Disponível em: <http://www.modulo.com.br/comunidade/articles/3074-a-cyberguerra-bate-em-nossa-porta>. Acesso em: 11/3/2015.

BRITTO, Carlos Ayres. **O Humanismo como Categoria Constitucional**. Belo Horizonte: Forum, 2012.

CANONGIA, Cláudia e MANDARINO, Raphael Júnior. **Segurança cibernética: o desafio da nova Sociedade da Informação.** In: Parcerias Estratégicas, Vol 14, número 29. Centro de Gestão e Estudos Estratégicos, Brasília, 2009.

CASTELLS, Manuel. **Redes de indignação e esperança: movimentos sociais na era da internet.** Trad: Carlos Alberto Medeiros. São Paulo: Zahar, 2013.

Debate: **Privacidade na rede** - Entre Aspas - Globo News Programa exibido em: 11/06/2013.

EL PAÍS. **Al Qaeda ameaça França com mais ataques.** Disponível em: <http://brasil.elpais.com/brasil/2015/01/10/internacional/1420882372_298511.html>. Acesso em: 11 03/2015.

FRANCE PRESSE. **FBI alerta para ameaças terroristas internas nos EUA.** Disponível em: <http://www.correiobraziliense.com.br/app/noticia/mundo/2014/11/03/interna_mundo,455817/fbi-alerta-para-ameacas-terroristas-internas-nos-eua.shtml>. Acesso em: 11 03/2015.

FRIEDMAN, Thomas L. **Quente, Plano e Lotado.** Trad.: Paulo Afonso. Rio de Janeiro:Objetiva, 2010.

GOCA. **Spring 2015 Conference.** Disponível em: <http://www.globaloffset.org/docs/GOCA%20Spring%202015%20Promotion%203-25-2015.pdf>. Acesso em: 27/3/2015.

GOOGLE. **Política de Privacidade.** Disponível em: <http://www.tecmundo.com.br/gmail/43257-google-revela-que-usuarios-do-gmail-nao-tem-nenhuma-privacidade.htm>. Acesso em: 15/3/2015.

INFOMONEY. **Comissão Europeia aconselha cidadãos a deixarem o Facebook.** Disponível em: < http://www.msn.com/pt-br/noticias/ciencia-e-tecnologia/comiss%C3%A3o-europeia-aconselha-cidad%C3%A3os-a-deixarem-o-facebook/ar-AAa71kh?ocid=mailsignoutmd>. Acesso em: 28/3/2015.

LA VANGUARDIA. **Irã sofre um ataque cibernético massivo.** Disponível em: <http://veja.abril.com.br/noticia/mundo/ira-sofre-um-ataque-cibernetico-massivo>. Acesso em: 15/3/2015.

MASI, Domenico de. **O Futuro Chegou.** Rio de Janeiro: Casa da Palavra, 2014.

MATSURA, Sérgio. **Bits e computadores no campo de batalha.** Disponível em: <http://www.modulo.com.br/comunidade/articles/3249-bits-e-computadores-no-campo-de-batalha>. Acesso em: 11/3/2015.

MORIN, Edgar. **Rumo ao abismo? Ensaio sobre o destino da humanidade.** Rio de Janeiro: Bertrand Brasil, 2011.

PORTAL TECMUNDO (RT). **Google revela que usuários do Gmail não tem nenhuma privacidade.** Disponível em: <http://www.tecmundo.com.br/gmail/43257-google-revela-que-usuarios-do-gmail-nao-tem-nenhuma-privacidade.htm>. Acesso em: 15/3/2015.

PORTAL VEJA. **Por que ficar atento aos novos termos de uso do google.** Disponível em: <http://veja.abril.com.br/blog/vida-em-rede/google/por-que-ficar-atento-aos-novos-termos-de-uso-do-google/>. Acesso em: 14/3/2015.

RAPOSO, Álisson Campos. **Terrorismo e contraterrorismo: desafio do século XXI.** in: REVISTA BRASILEIRA DE INTELIGÊNCIA. Brasília: Abin, v. 3, n. 4, set. 2007. Brasília : Abin, 2007.
RUIC, Gabriela. **Não espere privacidade ao usar o Gmail, diz Google.** Disponível em: <http://exame.abril.com.br/tecnologia/noticias/nao-espere-privacidade-ao-usar-o-gmail-diz-google>. Acesso em: 14/3/2015.

SAE/PR. **Setor Cibernético: Consultores apresentam metodologia para a elaboração de plano estratégico.** Disponível em: <http://www.sae.gov.br/site/?p=22350>. Acesso em: 10/3/2015.

TOGNOLLI, Claudio. **EUA podem endossar oficialmente tese de fraude eletrônica nas nossas eleições 2014.** Disponível em: <https://br.noticias.yahoo.com/blogs/claudio-tognolli/eua-passam-a-endossar-oficialmente-tese-de-fraude-151559066.html>. Acesso em: 15/3/2015.

YÁRNOZ, Carlos. **O terror jihadista coloca a França diante de um desafio histórico.** Disponível em: <http://brasil.elpais.com/brasil/2015/01/09/internacional/1420789660_177092.html>. Acesso em: 11 03/2015.

WAKEFIELD, Jane. **Entenda o ataque virtual à Sony.** Disponível em: <http://www.bbc.co.uk/portuguese/noticias/2014/12/141220_entenda_coreia_norte_lgb>. Acesso em: 11 03/2015.