Segurança e Privacidade na Internet

Fábio Luís Velloso, André Luis dos Santos Domingues
Pós Graduação em Rede de Computadores: Projeto e Implementação
Universidade Tecnológica Federal do Paraná (UTFPR)
Cornélio Procópio – PR – Brasil

Resumo: *O presente artigo tem por finalidade apresentar reflexões sobre as principais questões relacionadas ao acesso e proteção aos dados digitais e à privacidade dos usuários da rede e das Tecnologias de Informação correlatas. Com isto espera-se fornecer os subsídios essenciais para uma maior compreensão sobre as possibilidades de tratamento das informações e seu respectivo compartilhamento e divulgação, da importância da privacidade e os meios para se obter o mínimo de segurança na rede. A forma como os dados e informações devem ser tratados vão muito além do contexto dos sistemas, pois o impacto resultante do mau gerenciamento das informações podem afetar usuários, instituições e corporações em escala mundial. Dessa forma, torna-se importante uma abordagem que dê ênfase nas possibilidades e riscos existentes aos quais estão sujeitos estes dados e informações, bem como dos usuários envolvidos; independente de ser apenas um usuário doméstico, corporativo, institucional ou governamental: o que está em jogo nos dias atuais são o alto valor agregado das informações e o impacto trazido aos usuários.*

Abstract: *This article aims to provide some reflections on the issues related to access, protection of digital data and user's network privacy and Information Technology related. With this is expected to provide the essential information for a better understanding of the possibilities of information processing and its associated sharing and dissemination, the importance of privacy and the means to achieve the minimum network security. The way the data and information should be treated go far beyond of the context of the systems, because the impact resulted from the bad management of information can affect users, institutions and corporations worldwide. Thus, it becomes important an approach that emphasizes the possibilities and risks to which the data and information are subjected, as well as the users involved, whether it be just a domestic, corporate, institutional or governmental: what is at stake nowadays are the high value of information and the impact brought to users.*

1 INTRODUÇÃO

São vários os períodos da história humana onde pôde-se observar avanços de grande importância para o homem. Pode-se afirmar com toda a certeza que um grande número desses avanços fazem parte do grande sustentáculo que mantém nossa sociedade atual em pleno funcionamento. Mas o que tornou possíveis tais avanços certamente foi este: o surgimento da escrita e das formas de se registrá-la.

O surgimento da escrita serviu como base fundamental para o registro, o desenvolvimento e a propagação de todo o conhecimento nas sociedades humanas. Posteriormente tivemos a criação da imprensa e com isto todo o conhecimento passou a ser registrado em maior escala - livros, jornais, revistas, (para não falar de outras formas usadas)

o que proporcionou a ampliação da oferta de conhecimento e informação para um grande número de pessoas.

Nessas últimas décadas – com ênfase já nesse início do século XXI, com a criação, o desenvolvimento e a consequente evolução das tecnologias relacionadas à informática e a evolução das redes de dados – esta última fomentada diretamente pela necessidade de compartilhamento de recursos e informações, principalmente por parte de governos, universidades e demais instituições - possibilitou uma grande disseminação e aprimoramento das tecnologias desenvolvidas até então (serviços de e-mail, transferência de arquivos, compartilhamento de recursos de rede, listas de discussão etc).

Aliado a isso, tivemos também toda a questão da praticidade e facilidade centrada nos aplicativos, de forma a garantir aos usuários uma interação extremamente produtiva no tratamento das informações e recursos disponibilizados. Com tais aprimoramentos, tivemos também o desenvolvimento de novas tecnologias que tornassem possíveis uma maior segurança no compartilhamento dos dados gerados. Graças a todos estes fatores intrínsecos, pode-se hoje desfrutar de um sem-número de possibilidades oferecidas pelas Tecnologias da Informação.

Nos dias atuais, temos um número cada vez maior de pessoas, governos e instituições utilizando os serviços e recursos oferecidos pela Internet – independente da tecnologia ou plataforma utilizada. Nunca antes na história humana a informação e o conhecimento estiveram tão presentes na sociedade, de forma tão veloz e abundante como nos dias atuais.

Com isto, tivemos o surgimento de demandas relacionadas à proteção das informações e da privacidade de todos os usuários que utilizam os serviços disponibilizados nessa grande rede. Uma vez que uma vastíssima quantidade de informações sensíveis de usuários trafegam pela Internet a todo momento, tornou-se vital impedir que os mesmos usuários não sofressem com a utilização indevida de seus recursos computacionais e informações. Dessa forma, tivemos grandes esforços por parte de usuários, governos e instituições no sentido de intensificar os estudos ligados à segurança da informação e a respectiva privacidade do usuário.

2 ACESSO E PROTEÇÃO A DADOS DIGITAIS

Nos dias atuais, numa sociedade cada vez mais globalizada e altamente industrializada, torna-se praticamente impossível viver sem as vantagens e comodidades oferecidas pelas Tecnologias de Informação.

Todos os processos relacionados à oferta de produtos e serviços, encontram-se extremamente dependentes destas referidas tecnologias e encontram-se altamente conectadas[1].

Qualquer pessoa que tenha trabalhado com uma máquina de escrever e que alguma vez tenha organizado quaisquer tipos de documentos em pastas 'A – Z' em algum tipo de armário ou mesmo arquivando documentos em enormes arquivos de metal, sabe muito bem o quão trabalhoso era a manipulação dessas informações (sem contar que tais documentos poderiam ser facilmente perdidos).

Portanto, é um fato inquestionável de que as Tecnologias da Informação tiveram um forte impacto no que concerne a "nossa habilidade de criar, armazenar e compartilhar informação".

De forma subsequente, tivemos o grande *boom* na Internet, com a criação das redes sociais e o alto desenvolvimento do comércio eletrônico e a adesão cada vez maior por parte dos governos e demais instituições às vantagens e recursos oferecidos pela grande rede. Tudo isso trouxe um profundo impacto na forma das pessoas realizarem suas atividades e de se comunicarem[2].

Ainda nesse contexto, tivemos outra possibilidade tão impactante quanto as demais descritas anteriormente: o acesso a todas essas informações com apenas um click do *mouse.* Uma prova disso pode ser demonstrada a partir de situações tais como: uma compra qualquer efetuada através da Internet, num site que oferta produtos diversos; uma requisição no site do Detran para obter a Carteira de Habilitação (CNH) definitiva, uma consulta a eventos e apresentações culturais numa determinada localidade, entre outros.

Todas as informações destacadas acima foram obtidas sem sair de casa ou do trabalho, ou mesmo enquanto o usuário está em trânsito; tudo isso graças ao alto nível de conectividade atual à Internet, com acesso em tempo real a todos os dados e informações ali disponibilizados. Até mesmo a forma de nos comunicarmos foi afetada: antes usava-se enviar cartas a parentes e amigos usando os serviços dos correios; agora pode-se fazer a mesma coisa de forma extremamente rápida, usando e-mail ou mensagens instantâneas ou ainda fazendo uma postagem no Facebook. Tudo isso independente da plataforma utilizada – Desktop PC, Laptop, Smartphone ou Tablet.

Como pode-se observar, tudo o que se relaciona ao acesso e manipulação de informações tornou-se algo extremamente prático. Independente do tipo das informações ou

1 TORRES, Gabriel. Redes de Computadores. Novaterra. 2010

2 STEFANICK. Lorna. Controling Knowledge – Freedom of Information and Privacy Protection in a Networked World. AU Press. 2011.

da finalidade (se pessoal ou profissional) tudo pode ser acessado comodamente em nossas casas. Mas por meio destas atividades online outras pessoas podem obter nossas informações de maneira remota[3].

Temos agora uma situação bem delicada: o quanto de controle indivíduos e organizações devem ter sobre suas informações pessoais e corporativas? Quais tipos de informações podem ser acessíveis e quais devem ser restritas de forma a obter um nível adequado de privacidade?[4]

Tais questões tornam-se oportunas, uma vez que são dados e informações de usuários e instituições que estão em jogo. Sabe-se que estas mesmas informações podem ser usada de maneira imprópria, de forma a garantir os interesses escusos de certas pessoas e instituições, em detrimento aos interesses e privacidade de outras pessoas e instituições. Atualmente, um grande número de instituições e governos se deram conta da importância de resguardar seus dados e informações, e raros são os usuários comuns que possuem uma visão mais ampla de como a segurança de suas informações e suas própria privacidade no contexto da Internet são importantes.

A liberdade de acesso às informações e a proteção à privacidade tornaram-se questões amplamente discutidas atualmente, pois trazem impactos de amplo alcance regional e mundial. Isto apresenta alto nível de criticidade, uma vez que tais fatores influenciam na maneira como a sociedade se comporta, em âmbito econômico e democrático e a presença da relação existente entre privacidade e autonomia.

Para se ter uma ideia mais exata desta questão, Fred H. Cate[5] destaca vários exemplos de informações e dados pessoais que podem ser coletados e cruzados a partir de nossas próprias atividades no cotidiano:

a) Bancos, Hospitais e Cartórios possuem informações sobre todo o nosso histórico financeiro, de saúde e familiar;

b) Empresas de Telecomunicações possuem todas as listas dos números de telefone mais usados, tempo de conversação, frequência das ligações e teor das conversas;

c) Operadoras e administradoras de cartão de crédito possuem todos os perfis de consumo relativos aos seus clientes, bem como de seu histórico de compras;

d) Editoras possuem informações relativas ao hábito de leitura de seus assinantes;

---

3 MUNGO, Paul. GLOUGH, Bryan. Approaching Zero – The Extraordinary World of Hackers, Phreakers, Virus Writers and Keyboard Criminals. Random House. 1992.

4 STEFANICK. Lorna. Controling Knowledge – Freedom of Information and Privacy Protection in a Networked World. AU Press. 2011.

5 CATE, Fred H.Privacy in the information age. Washington: Brookings, 1997.

e) Lojas e demais estabelecimentos comerciais detém cadastro de seus clientes e respectivo histórico de consumo, possibilitando a criação de listas de compras personalizadas para cada tipo de cliente;

f) Provedores de acesso à Internet possuem registro dos acessos efetuados a sites, frequência e tempo de acesso, conteúdo visualizado, entre outros.

Todas as possibilidades destacadas acima remetem ao caráter essencialmente prático e de alta velocidade que a evolução das Tecnologias de Informação nos trouxeram. Todas as informações a partir daí, farão parte de um gigantesco banco de dados. Pode-se então ter acesso a todas as características, hábitos e práticas de milhares de pessoas, de forma a revelar certos aspectos e facetas dos indivíduos até então desconhecidos – às vezes aspectos desconhecidos até mesmo para o próprio indivíduo em questão. Além do uso dessas bases de dados para fins comerciais, as mesmas podem ser utilizadas por órgãos do governo e demais entidades públicas ou privadas, inclusive para fins de processo criminal.

Dessa forma, Reinaldo Demócrito Filho[6] afirma:

> "(...) se, por um lado, a coleta de informações pessoais pode favorecer negócios, facilitar decisões governamentais ou mesmo melhorar a qualidade de vida material da sociedade como um todo, outros valores precisam ser considerados à luz da privacidade individual."

Da afirmação, podemos inferir que tais práticas também se constituem como um problema sócio-jurídico, sendo necessário delimitar até que ponto as mesmas podem ser exercidas e quais as formas adequadas de se fazê-la, de forma a não incorrer em violação de privacidade.

Segundo Pablo Stolze (2003, p. 106):

> "Com o avanço tecnológico, os atentados à intimidade e à vida privada, inclusive por meio da rede mundial de computadores (Internet), tornaram-se muito comuns. Não raro determinadas empresas obtêm dados pessoais do usuário (profissão, renda mensal, hobbies), com o propósito de ofertar o seus produtos, veiculando a sua publicidade por meio dos indesejáveis spams, técnica ofensiva à intimidade e à vida privada."

Portanto, tais questões demandam um alto nível de atenção, uma vez que torna-se evidente a alta velocidade de evolução das tecnologias da informação e das formas de armazenamento, compartilhamento e disseminação das informações; e tudo isso requer uma

---

6 REINALDO FILHO, Demócrito (coord.). Direito da Informática – temas polêmicos. 1a Ed., Bauru, SP: Edipro, 2002.

consideração mais cuidadosa de como gerenciamos nossas informações. Decisões pertinentes ao fato de conservar ou compartilhar informações particulares sempre tiveram um grande impacto em indivíduos e organizações; e isso tem se refletido de forma bastante significativa nos dias atuais, principalmente para governos, instituições e corporações.

Num mundo cada vez mais globalizado e digitalizado, todas as nossas escolhas referentes à maneira como gerenciamos informações, influirão de forma vital na definição e evolução de nossa própria sociedade[7].

3 PRIVACIDADE

3.1 Legislação

O atual panorama brasileiro, no que concerne às leis e regulamentos no âmbito da rede, ainda demonstram inadequação no que diz respeito à proteção de dados. A proteção dos dados dos usuários é tratada de maneira não específica; esta proteção está diretamente relacionada à privacidade e à transparência na rede, mas sem qualquer proteção aos dados em si.

Com relação ao fato exposto, pode-se observar na Constituição Federal (CF 1988) no Artigo 5º. todo um conjunto de direitos, esses tidos como fundamentais e sendo assegurada a sua garantia a todo cidadão. Pode-se observar a presença de vários tipos de provimentos relacionados à proteção dos dados e à privacidade, tais como o *habeas data* e a inviolabilidade nas comunicações.

Ainda tratando do texto constitucional, temos disposto no inciso X do artigo em questão que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". Ainda que esta citação seja o bastante para garantir a privacidade das pessoas, o texto dá margens para várias interpretações; com isto, não se obtém um texto que faça um tratamento realmente efetivo e inteiramente específico no tocante à proteção de dados.

No contexto mundial, o Poder Judiciário no Brasil possui certo nível de participação na discussão sobre tais questões. Um exemplo disso é a ampliação do conceito de espaço público, o que garante a ampliação do direito à privacidade, ainda que isto tenha aplicado certas limitações à liberdade de expressão. Apesar disso, o Brasil encontra-se bastante vulnerável em termos de legislação em relação a outros países.

---

7 STEFANICK. Lorna. Controling Knowledge – Freedom of Information and Privacy Protection in a Networked World. AU Press. 2011.

Nesse sentido, o Anteprojeto Brasileiro de Proteção de Dados Pessoais trata destes aspectos distintos e "dispõe sobre a proteção de dados pessoais, a privacidade e dá outras providências", estabelecendo assim uma correlação com as legislações estrangeiras (A Diretiva Europeia de Proteção de Dados Pessoais (EC 95/46) e a Lei de Proteção de Dados Canadense).

Deve-se abordar que esta norma também discorre sobre dados sensíveis, dados estes que podem estar inseridos numa esfera de confidencialidade. Com isto, tem-se uma demanda no sentido de incluir os aspectos relativos à intimidade, de forma a estar congruente com o Artigo 5º., inciso X da Constituição Federal de 1988, e demais estudos que venham a fazer a distinção entre segredo, intimidade e privacidade. (HUBMANN *apud* COSTA JÚNIOR, 2007). O Anteprojeto ainda traz ao conhecimento os conceitos de "banco de dados", "dado pessoal", "comunicação", "dados sensíveis", "difusão" dentre outros.

Verifica-se a necessidade de um maior nível de profundidade em certos artigos e incisos, principalmente dos que tratam da segurança em repositórios de dados – públicos e privados – e daqueles que fazem menção à titularidade dos dados. Julga-se fundamental a criação de um órgão regulatório, de caráter autônomo. Entretanto, o texto normativo guarda certa congruência com o Código Civil, determinando assim que atividades na rede representam atividades de risco, sendo portanto passíveis de responsabilidade objetiva.

O Anteprojeto conta com dez princípios norteadores, nos quais fundamentam-se o caráter didático e reiterando as bases para as demais previsões da norma, lembrando que a aplicação dos princípios constantes da referida norma decorrem fatalmente do Código Civil e do Texto Constitucional, não sendo necessárias previsões específicas.

Portanto, podemos depreender que o surgimento e a proliferação de novas tecnologias, aliadas ao crescimento da oferta de conexões à Internet no país acaba por criar uma certa pressão no sentido de elaborar leis e diretivas que regulamentem o comportamento dos usuários na rede.

Assim sendo, o Anteprojeto representa não somente a proteção dos dados pessoais mas sim a criação de um modelo jurídico que sirva de suporte ao desenvolvimento tecnológico, otimizando todas as relações de consumo na sociedade.

Mas existe algo importante a ser considerado na conjuntura do Marco Civil da Internet: a liberdade. Sempre que temos a presença de termos como "regulamento" é mais que evidente que existe uma necessidade implícita por parte do estado de controlar e manipular as operações existentes no âmbito da grande rede. Por mais que a letra da lei seja bem intencionada, sempre existe – e isto do ponto de vista jurídico é exaustivamente provado – a

possibilidade de mudança interpretativa; sempre onde houver esse tipo de “brecha” na lei, o governo – mais que prontamente – irá exercer domínio. Isto por si só já representa uma grande ameaça não só à liberdade, como também da própria privacidade e segurança das informações de todos os usuários e entidades envolvidas.

Neste sentido, o Marco Civil da Internet acaba por tornar-se uma ameaça, por ser um projeto que pode ferir os direitos e liberdades dos usuários dos serviços de rede. A Internet proporciona todas as possibilidades de liberdade democrática para seus usuários e o Estado através de um marco regulatório pode, nesse sentido, restringir e controlar o que é feito ou visto na Internet. A Internet – e todos os recursos disponíveis – podem se auto-regulamentar, por meio dos próprios usuários e das empresas de tecnologia, conforme forem surgindo demandas e especificidades relacionadas.

3.2 Transparência e Privacidade

Com os rápidos avanços no campo das Tecnologias da Informação aliados à expansão vertiginosa da Internet ocorridos durante o século XX e estendendo-se aos dias atuais, pôde-se verificar que parte dos usuários e instituições envolvidos acabaram por constatar que a chamada “privacidade” em toda a extensão do termo, encontra-se praticamente inexistente. Isso se deve ao volume imenso de informações que encontram-se transitando na rede por meio das Tecnologias da Informação. Tudo isso acaba por impossibilitar a salvaguarda de informações e fatos ocorridos no âmbito pessoal, profissional e Institucional.

Diante de tais informações, a mera declaração de que a privacidade “está morta” pode ser tomada com grande preocupação. A despeito da Internet ser um ambiente virtual, este mesmo sustenta-se e está inteiramente fundamentado na existência de fatos reais.

Com a grande intensificação no volume de informações e a massificação das Tecnologias da Informação acabou por criar um termo bastante difundido atualmente: a “sociedade da informação”, ou “era da informação”. Conforme declara Manuel Castells, a sociedade que surge dessa “revolução tecnológica” é a chamada “sociedade em rede”, cuja característica encontra-se fundamentada na não centralização das informações e pela aplicação dessas informações para gerar conhecimento e novas tecnologias, num constante processo de realimentação cumulativa.

Nesse sentido, nota-se claramente as possibilidades trazidas pela Internet e pelas Tecnologias da Informação no tocante à criação e disseminação de conteúdo pela rede, desenvolvendo-se dessa forma uma sensação de controle sobre tais tecnologias. Tal sensação

de controle torna-se extremamente atraente, mas demanda um estudo e análise de todos os potenciais e problemas decorrentes da manipulação dos dados e informações.

Por tratar-se de questões que vão muito além do âmbito "virtual", a livre disseminação de informações carrega em si possibilidades – isso é fato – mas também uma série de problemas que abrangem toda a esfera e realidade sociais, que podem ocasionar grande impacto aos usuários e instituições. Todas as atividades humanas – de alcance econômico e social, por exemplo – são amplamente conhecidas e difundidas, tornando visíveis um mundo por vezes repleto de escândalos, discussões polêmicas, corrupção, espionagem, entre outros.

Nesse contexto, transparência e privacidade apresentam-se como conceitos-chave, extremamente críticos à liberdade de expressão numa sociedade democrática.

Conforme destaca Lorna Stefanick (2011, p.8):

> "Access to information legislation is based on the concept of transparency. Through scrutiny of behavior and performance, people are held accountable for their actions. Transparency also allows visibility for the curious, however, or visibility for reasons other than ensuring accountability. It thus becomes an important counterpoint to privacy".

Ainda nesse sentido, David Heald "*(...) provides a typology for undestanding the different directions in which transparency can flow: upwards, downwards, inwards, and outwards".*

A partir do exposto, quando se fala em transparência, tem-se claramente o tipo de comportamento a ser considerado no âmbito da rede e as relações existentes nesse contexto, entre as partes envolvidas e os tipos de fluxos de dados a serem considerados nesse ambiente.

Privacidade, assim como Transparência, apresenta-se como um conceito bastante abrangente. Constitui-se de quatro componentes, intrínsecamente relacionados: Privacidade Física, Privacidade nas Comunicações, Privacidade territorial e da Informação. A Privacidade Física está diretamente ligada ao caráter pessoal, de forma a garantir a integridade física dos indivíduos contra todo e qualquer procedimento invasivo que comprometa a individualidade e a própria vida do indivíduo.

A Privacidade nas Comunicações torna possível uma cobertura ampla nos aspectos relacionados à privacidade e segurança em e-mails, correspondências convencionais, ligações telefônicas entre outras formas de comunicação. Privacidade Territorial está ligada ao estabelecimento de parâmetros e limites no que diz respeito à invasão de espaços físicos – não importando qual seja o tipo – locais de trabalho e residências se encaixam nessa nomenclatura. Privacidade da Informação está relacionada à manipulação e armazenamento

de dados pessoais ou particulares. Tais informações encontram-se em grandes bases de dados – Cadastros de clientes em centrais de cartão de crédito, registros médicos em clínicas e postos de saúde e demais entidades, sejam elas governamentais ou particulares.

Pode-se depreender a partir das informações apresentadas, que os conceitos "Transparência" e "Privacidade" estão intimamente ligados. Para alcançar uma compreensão sobre o tema, pode-se destacar os últimos incidentes ocorridos com os dados sigilosos do governo brasileiro e da própria presidente, por meio de espionagem norte-americana na rede. Tais incidentes, envolvendo o uso de técnicas de espionagem e contra-espionagem, também são recorrentes em outros países, ainda que não venham ao conhecimento do público, e demandam uma abordagem centrada na correta utilização dos recursos disponíveis das Tecnologias de Informação e da Internet. Uma vez que processos de espionagem, monitoramento e invasão de sistemas causam grande impacto tanto para governos e empresas, como também para usuários comuns.

3.3 Proteção da Privacidade

É importante destacar o termo Privacidade fazendo uma abordagem de suas origens e respectiva evolução. Quando considera-se a origem do termo, o mesmo não teve o seu surgimento ligado em momento simultâneo ao de outros direitos. Dessa forma, não foi de imediato reconhecido nos Códigos Civis ou Constituições no decorrer do século XIX; somente fora reconhecido em âmbito legislativo somente no século XX.

A partir do momento do surgimento de novas tecnologias que impactaram diretamente na forma como era feito o acesso e divulgação de informações, e fatos ligados à privacidade, acabaram por impulsionar os debates acerca destas questões. Um exemplo pioneiro nesse sentido é o famoso artigo que fala sobre privacidade, publicado na *Harvard Law Review*, intitulado "*The Right to Privacy"*, de Samuel Warren e Louis Brandeis, em dezembro de 1890. Nesse trabalho, os autores discorrem sobre como o advento de certos aparatos tecnológicos, tais como Jornais e a fotografia invadiram de forma consistente os domínios da vida privada. O documento é uma alusão clara ao direito de privacidade, partindo de diversos precedentes jurisprudenciais.

Com este tipo de fundamentação, o direito à privacidade, Warren e Brandeis relacionaram a sua proteção ao conceito de inviolabilidade da personalidade. Nas palavras dos autores, "o princípio que protege escritos pessoais e outras produções pessoais, não contra o

furto ou a apropriação física, mas contra toda forma de publicação, é na realidade não o princípio da propriedade privada, mas da inviolabilidade da personalidade".

Com isso, o artigo ressalta um fato até então inédito: identificando a privacidade como um direito e fundamentando este na proteção da personalidade, demonstrando a importância desse direito mesmo em face aos avanços tecnológicos e o respectivo reconhecimento desse direito em futuras gerações, como um direito constitucional.

O artigo deixa clara a ideia da proteção à privacidade como sendo algo bastante particular e íntimo, com foco bastante individualista. Concepção que acabou por transformar-se em pressuposto de forma a reconhecer outros direitos fundamentais. Portanto a violação de privacidade, nos dias de hoje, possui um alcance muito maior, afetando grande número de pessoas e instituições.

Na sociedade atual, é comum nos depararmos com situações bastante diversas que, de forma direta ou indireta afetam a nossa privacidade e divulgação de informações. Quem nunca passou por situações em que fomos filmados ou fotografados sem nosso consentimento? Câmeras espalhadas aos quatro cantos de um recinto ou mesmo uma cidade, mas que sequer são capazes de garantir realmente um nível de segurança efetivo. Tais indagações levam a crer que existe um problema sério, tanto em nível de segurança quanto de privacidade.

A Internet já faz parte de nosso cotidiano. Dadas às inúmeras facilidades e a uma profusão quase que infinita de informações, de todos os tipos e para todos os gostos, provavelmente seria muito difícil viver, ou sequer imaginar em como seria a vida sem todas as comodidades e recursos fornecidos pela Internet.

Graças à Internet podemos fazer e encontrar novos amigos, estar em contato com familiares distantes, participar de cursos à distância, acessar sites de notícias, realizar serviços bancários, pagamentos de contas; enfim, um sem-número de possibilidades. Isso são apenas alguns exemplos de utilização da Internet. Mas para que todo esses recursos sejam aproveitados de forma plena e segura, certas precauções e cuidados são altamente recomendados, de forma a reduzir os riscos à exposição na rede.

Nessa abordagem, podemos destacar alguns dos riscos existentes na grande rede, tais como:

*** Acesso a conteúdos impróprios ou ofensivos:** durante a navegação, o usuário pode ter contato com sites que hospedem páginas de conteúdo pornográfico ou que possam atentar à horar e incitar o ódio e o racismo.

*** Roubo e perda de dados:** Todas as informações presentes em seus dispositivos, sejam computadores, laptops e outros dispositivos móveis que estejam conectados à Internet podem ser apagados ou roubados, através da ação de crackers que executam códigos maliciosos nas máquinas a serem atacadas;

*** Invasão e perda de privacidade:** Informações pessoais divulgadas comprometem a privacidade. Mesmo restringindo seu acesso, não há garantias de que as mesmas não serão repassadas, haja visto que sites que possuem suas próprias políticas de privacidade podem fazer sua alteração sem prévio aviso ao usuário; tornando o que era privado em público;

*** Problemas com o sigilo das mensagens:** Na Internet, se não forem tomadas as devidas precauções, as informações que trafegam podem ser interceptadas ou armazenadas em outros locais;

*** Violação de Direitos Autorais:** Todo e qualquer procedimento que envolva cópia, distribuição ou alteração de materiais de conteúdo protegido pela Lei de Direitos Autorais podem constituir-se em problemas de ordem jurídica, implicando em perdas financeiras.

Como pode-se observar, os riscos relacionados ao uso da Internet são vários; citamos apenas alguns. Mas nenhum deles se iguala a este: o de supor que ninguém tem interesse em utilizar o seu computador. É mais do que provado que os crimes virtuais em grande parte se devem ao fato do atacante possuir um grande número de computadores sob seu controle, infligindo ataques de grandes proporções.

Todos estes fatores causam grande impacto na privacidade e segurança das informações de usuários e organizações, colocando em risco a integridade e confidencialidade das informações, sem contar na alta taxa de disseminação de códigos maliciosos e spam.

Como forma de mitigar tais riscos, deve-se levar em consideração que a Internet é um ambiente de interação humana, com todas as premissas e possibilidades envolvidas. A Internet é "virtual" apenas em teoria; na prática, todas as interações são totalmente reais, pois usuários, instituições e governos interagem nesse ambiente e todos possuem existência fora da Internet.

Portanto, todos os entes envolvidos estão sujeitos a riscos e tentativas de golpe bastante semelhantes as que ocorrem em outros meios, como na rua ou por telefone por exemplo[8].

No cotidiano da rede, é necessária uma abordagem mais preventiva. Todos os cuidados e precauções que teríamos no dia a dia no "mundo real", pode e devem ser repetidos

8 KLEINIG, John. et al. Security and Privacy – Global Standards for Ethical Identity Management in Contemporary Liberal Democratic States. Washington: Brookings, 1997.

em ambiente virtual. Uma postura preventiva garante a segurança e a mesma deve ser incorporada à própria rotina; não importando o local, o contexto ou tecnologia utilizada.

Outra forma de garantir a segurança das informações e a privacidade dos usuários é possuir a garantia de que os serviços de rede disponibilizados ofereçam requisitos básicos de segurança, tais como:

* **Identificação:** Uma entidade deve necessariamente se identificar, ou seja, dizer quem ela é.
* **Autenticação:** Deve ser verificável se a entidade em questão é quem ela afirma ser.
* **Autorização:** Identificar e determinar quais ações e procedimentos a entidade em questão pode executar.
* **Integridade:** A proteção da informação contra alterações não autorizadas.
* **Confidencialidade:** Proteger a informação contra acessos não autorizados.
* **Disponibilidade:** A garantia de que determinados recursos estejam sempre disponíveis.
* **Não repúdio:** Uma entidade não pode negar que foi ela quem executou uma determinada ação.

Como pode-se observar, todos os procedimentos que estejam relacionados à privacidade e segurança na Internet, estão diretamente relacionadas ao próprio comportamento dos usuários dos serviços de rede. Todo e qualquer ato que envolva a utilização das Tecnologias de Informação disponíveis para acesso à rede devem partir dos princípios que norteiam todo o cerne em questão: Integridade, Confidencialidade e Disponibilidade.

3.4 Proteção de Dados e Segurança da informação no Brasil

Num contexto mundial, o Brasil não possui normas e regulamentos que disponham sobre a proteção de dados pessoais. Ainda que consideremos os direitos de proteção à intimidade e à privacidade garantidas pela Constituição Federal e pelo Código Civil, o Brasil

ainda encontra-se muito aquém do nível de organização de outras legislações, como as da Argentina, Estados Unidos, Europa e México[9].

Como forma de efetuar as adequações necessárias, foi criado o Anteprojeto de Lei de Proteção de Dados Pessoais, tendo por base outras legislações existentes em âmbito internacional, como a Diretiva Européia de Proteção de Dados Pessoais (EC 95/46) e a Lei de Proteção de Dados Canadense; com tais esforços, busca-se reduzir a grande quantidade de falhas de segurança e a consequente perda ou roubo de informações.

O conceito de Proteção de Dados digitais, de forma geral, remete às próprias origens dos processos que culminaram no pleno uso e armazenamento de informações. Dada a utilização maciça de dados e informações, associadas ao processo de burocratização de instituições públicas e privadas e ao desenvolvimento das Tecnologias da Informação no decurso do século XX[10].

Todos estes fatores proporcionaram não só o desenvolvimento vertiginoso dos processos relacionados à organização e sistematização de dados e informações de governos e instituições, como também a necessidade de garantir a proteção destas informações.

A possibilidade de combinar as mais variadas técnicas de automatização tornou possíveis o desenvolvimento de todas as funções de coleta de dados, seu respectivo armazenamento, organização e transmissão de dados de tal forma nunca antes vista ou imaginada. Tudo isso trouxe possibilidades fantásticas para a sociedade, o que acabou por influenciar todos os ramos de atividade humana, sejam elas de cunho social, político ou econômico[11].

As informações a partir de então acabaram por adquirir alto valor agregado, pois aumentaram o número de possibilidades para a formação de novos elementos informacionais que venham a oferecer mais detalhes acerca dos processos que influam direta ou indiretamente na vida de cidadãos e entidades diversas[12].

Um exemplo clássico das possibilidades existentes nesse contexto, pode-se destacar a técnica de criação ou construção de perfis sociais em redes de relacionamento por exemplo.

---

9 LIMA, Caio Cesar Carvalho. MONTEIRO, Renato Leite. Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada. <http://www.atoz.ufpr.br/index.php/atoz/article/view/41>.

10 BENNETT, Colin. Regulating Privacy: data protection and public policy in Europe and the United States. Op. Cit., p. 43.

11 ALCALÁ, Humberto Nogueira. Autodeterminación informativa y hábeas data em Chile e información comparativa. In: Anuário de Derecho Constitucional Latioamericano 2005, Tomo II, Konrad Adenauer Stiftung, p. 449.

12 DE LA CUEVA, Pablo Lucas Murillo. La construcción del derecho a la autodeterminación informativa. In: Revista de Estudios Políticos ,104 (Nueva Época), Abril/Junio 1999, Madri, p. 38

A partir das informações ali presentes podem ser tomadas uma série de decisões a respeito de quais serviços oferecer ou propagandas a apresentar aos usuários; tudo isso traz certo nível de impacto na privacidade do usuário, influenciando o seu acesso a determinadas oportunidades sociais.

Como evidencia Perez Luño, na atual sociedade todos os tipos de informações convertem-se em poder, desde o instante em que as Tecnologias permitam transformar partes dispersas de informações em um bloco único e organizado de informação.

Considerando tais questões, pode-se compreender perfeitamente que as Tecnologias de Informação disponíveis atualmente são responsáveis por toda a organização do aparato de informações de usuários, governos e instituições.

As informações, portanto, necessitam ser protegidas das várias ameaças existentes, garantindo assim continuidade do negócio, mitigar os riscos e maximizar o retorno sobre os investimentos e oportunidades de negócios. A partir da implementação de um conjunto de controles – processos, políticas, procedimentos, funções de hardware e software – os objetivos de segurança da informação podem ser alcançados.

Conforme consta da Norma ABNT NBR ISO/IEC 17799:2005 (2005, p. 9):

> "A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades".

Na atual conjuntura brasileira, a segurança da informação torna-se crítica, tanto no setor público como no setor privado, proporcionando um nível adequado de proteção das infraestruturas críticas.

Com o alto nível de interconexão existente, tal abordagem torna-se oportuna, pois independente dos setores da sociedade a serem considerados (público ou privado) ambos possuem a necessidade de viabilizar as oportunidades de negócios, seja o próprio governo (*e-gov*) ou comércio eletrônico (*e-business*).

Sendo assim, quando se questiona a segurança da informação, o foco recai sobre a Norma ISO/IEC 17799:2005, fornecendo as técnicas e códigos necessários à gestão da Segurança da Informação. Mas quando se trata da Proteção de Dados percebe-se ainda uma certa necessidade de se adaptar e reformular certos aspectos presentes no referido projeto, de forma que o mesmo guarde um certo nível de confluência com a Constituição Federal.

4 SEGURANÇA E PRIVACIDADE NA INTERNET: ESTUDOS DE CASO E COMENTÁRIOS

Computadores, por sua natureza e funcionalidade, processam dados; dados estes que, sistematizados e organizados convertem-se em informação. Estas informações podem atender a diversas finalidades. Na esfera computacional, tais informações podem ser combinadas, agregadas, coletadas, pesquisadas; enfim, pode-se inferir as mais variadas formas de processamento. Uma vez que as informações estejam inseridas e organizadas por meio destes parâmetros, estão prontas para serem propagadas por meio da rede.

Obviamente, toda e qualquer pessoa ou instituição pode fazer uso destas informações. Isso é premissa básica para toda e qualquer decisão a ser tomada, independente do contexto a ser considerado – seja no âmbito particular ou público.

O governo, por exemplo, necessita de determinadas informações sobre certos indicadores sociais e econômicos, de forma a efetuar os estudos necessários à criação e implementação das respectivas medidas sócioeconômicas. Companhias de seguro necessitam saber a quais tipos de risco uma determinada pessoa está sujeita, por meio de informações sobre seu estilo de vida, histórico médico e possíveis doenças entre outros. Empresas desejam conhecer e obter informações sobre os hábitos de consumo dos consumidores. Com as informações necessárias, as empresas podem elaborar estratégias que venham a influenciar todo o processo de oferta e procura de produtos e serviços.

Pode-se ainda destacar a esfera pessoal, onde os pais de uma criança, no momento da matrícula em uma escola, desejem saber sobre o projeto político-pedagógico empregado na escola e se o mesmo está de acordo com os princípios democráticos e éticos vigentes. Portanto, é bastante comum as pessoas buscarem informações acerca de parentes e amigos, saber onde estão e o que estão fazendo, bem como sobre pesquisar sobre os mais variados assuntos e interesses.

Não há dúvidas sobre os benefícios proporcionados pelos computadores. Até duas décadas atrás, sequer se imaginava o leque tão vasto de possibilidades a serem explorados. E ainda deve-se considerar o surgimento das tecnologias que impactaram na criação das redes de computadores. Computadores tornaram possível combinar a informação de várias formas e as redes de computadores proporcionaram o

compartilhamento dessa informação e dos recursos disponíveis. A partir do desenvolvimento e evolução das Tecnologias da Informação e melhoria na oferta de produtos e serviços relacionados a tais tecnologias, tivemos o surgimento de novos serviços: melhorias nos mecanismos de busca e pesquisa, comércio eletrônico, redes sociais, blogs, cursos online entre outros.

Com este infinito conjunto de possibilidades, surgem grandes questões. Até que ponto as informações podem ser compartilhadas e qual deve ser o nível de proteção para informações particulares ou confidenciais. Nesse oceano de possibilidades, as informações passaram a ter grande valor agregado. Independente do usuário em questão, tem-se agora um grande conflito em torno do uso e armazenamento das informações *versus* sua proteção.

A proposta deste estudo é uma abordagem das formas de uso e de manipulação que a informação assume em determinadas situações, tendo como pano de fundo a utilização das Tecnologias da Informação e das redes de dados; discutindo acerca do valor e da importância da privacidade e da segurança da informação, e observando sempre que possível as implicações legais.

Marco Civil da Internet

Conforme destacado por CGI.br, "O Marco Civil da Internet é um projeto de Lei que visa a consolidar direitos, deveres e princípios para a utilização e o desenvolvimento da Internet no Brasil". A proposta surgiu da iniciativa conjunta da Secretaria de Assuntos Legislativos do Ministério da Justiça e o Centro de Tecnologia e Sociedade da Escola de Direito da Fundação Getúlio Vargas no Rio de Janeiro. Tal iniciativa teve por base a Resolução CGI.br/RES/2009/003/P cujo título é "Os princípios para governança e uso da Internet".

As fases iniciais deste processo, divididas em eixos de discussão, foram propostas à sociedade, com temas e debates sobre o uso da Internet. Foi inclusive criado um *site* na Internet, dedicado especificamente a receber as contribuições – comentários, propostas e mensagens diversas – vindos dos mais diversos setores da sociedade. Após concluída esta fase, formulou-se a minuta do anteprojeto, para que fosse apresentada à sociedade, de forma a possibilitar o debate acerca do assunto. Todo os debates e interações feitas vieram a dar origem ao Projeto de Lei 2.126/2011 (PL 2126) a ser apresentado à Camara dos Deputados.

Com isto, o Brasil passa a ganhar notoriedade e repercussão internacional, visto que tal documento passaria a definir quais os princípios de uso da Internet no Brasil, enfatizando o caráter livre e aberto para a Internet e a garantia do cumprimento das regras para a proteção do usuário e o papel dos Provedores de Internet e das Empresas de Telecom.

No referido Projeto de Lei, no Capítulo II – Dos Direitos e Garantias dos Usuários, Artigo 7º. Inciso I, destaca o direito "À inviolabilidade e ao sigilo de suas comunicações pela Internet, salvo por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução preocessual penal". E o artigo 8º. fornece "A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à Internet".

Certos aspectos no presente projeto de lei chamam a atenção pelo fato de abrir possibilidades para outras interpretações. Um exemplo disso é que o usuário dos serviços de Internet está sujeito a ter seus dados de conexão armazenados pelos provedores por um período de um ano. Até aqui, sem problemas; provedores de Internet armazenam os *logs* contendo tais informações, que se restringem somente ao registro de conexão – data e hora de início e término da conexão, sua duração e o endereço IP utilizado pelo terminal.

Não é permitido ao provedor efetuar qualquer tipo de monitoramento que venha a violar a privacidade e o sigilo dos dados trafegados, de forma que este registro não conterá quais os sites acessados e as aplicações envolvidas – até porque seria um problema para o provedor manter um registro completo destas informações.

No artigo 12, temos que "Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de Internet". Mas o artigo 13 destaca que "Na provisão de aplicações de Internet é facultado guardar os registros de acesso dos usuários, respeitando o disposto no artigo 7º.", acabar por tornar sem efeito o artigo 12, uma vez que os registros de acesso às aplicações de Internet serão armazenados e utilizados para fins de investigação criminal ou instrução processual penal; isso se justifica para os fins considerados, ou seja, em termos jurídicos.

Mas isso abre precedente para que o próprio governo tome posse destas informações, conforme leitura do parágrafo 3º. do artigo 13 do referido projeto de lei: "(...), a autoridade policial ou administrativa poderá requerer cautelarmente a guarda dos registros de aplicações de Internet, observados o procedimento e os prazos previstos nos parágrafos 3º. e 4º. do artigo 11".

A 'autoridade administrativa' neste parágrafo entra como um 'cavalo-de-tróia', pois a privacidade e liberdade de expressão são garantias contitucionais; com isto, torna-se evidente o interesse do governo em controlar as atividades dos usuários na rede, ferindo direitos constitucionais.

Outra questão abordada pelo Marco Civil é sobre a neutralidade da rede. Esse princípio destaca que para toda e qualquer informação que trafega na rede que a mesma seja tratada da mesma forma, não influindo ou prejudicando a navegação em termos de velocidade. Com isto, a neutralidade da rede também fornece as garantias necessárias para que todas as informações possam ser acessadas livremente, sem qualquer tipo de restrição baseada no tipo de protocolo de rede utilizado.

No contexto do Marco Civil, a questão da neutralidade da rede acabou por gerar uma certa polêmica, pois em determinado momento cogitou-se a possibilidade de criar regras mais flexíveis; onde as empresas de telecomunicação teriam a liberdade de oferecer serviços de forma diferenciada. Basicamente, isso implica em dar prioridade a determinados serviços em detrimento de outros. Isso acaba não fazendo qualquer sentido prático ou mesmo comercial, pois durante uma navegação usual, não se acessa somente uma parte da rede.

Considerando tais inconsistências, o texto do projeto que tratava especificamente dessa questão foi reformulado, conforme temos no art. 9°.: “O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicativo”. Com isto, a discriminação de serviços e tipos de dados trafegados somente sofrerá interferência se houver a necessidade de cumprimento de requisitos técnicos para a operação adequada das aplicações e dos serviços relacionados. Somente em situações específicas as empresas de telecom poderão valer-se da prerrogativa em questão.

Quando desta situação, os usuários dos serviços devem ser notificados sobre os motivos que levaram à priorização de determinado tráfego, com todos os mínimos detalhes técnicos e explicações correlatas.

O Marco Civil da Internet representa um passo importante, não para a regulamentação formal que visa interesses de determinados grupos e governo, mas como forma de proteger a privacidade e inviolabilidade das informações, bem como do sigilo das mensagens.

ONU e a proteção da privacidade na Internet

Com as recentes polêmicas sobre as declarações de Edward Snowden, ex-analista de segurança da NSA (*National Security Agency*) do governo norte-americano, acabaram por gerar incômodo e preocupação generalizada por parte de cidadãos comuns e governos mundiais.

Segundo denúncias fornecidas por Snowden, o governo norte-americano tem feito uso de técnicas de monitoramento intrusivas, de alcance global e de forma bastante ostensiva. O monitoramento e vigilância se estende a milhares de cidadãos nos Estados Unidos e de outros países, bem como de outros governos ao redor do mundo.

É evidente que os danos causados pelas práticas denunciadas por Snowden trazem um impacto muito mais profundo e significativo do que qualquer discussão sobre segurança da informação e privacidade possam revelar.

Como forma de contrapor as incursões norte-americanas, os governos do Brasil e da Alemanha – ambos espionados pelos EUA – combinaram esforços e apresentaram durante a Assembléia Geral da ONU uma proposta de resolução que venha a reconhecer o direito à privacidade no âmbito internacional.

O documento conta com o endosso de mais 21 países e ganhou força após novas denúncias de Snowden para o Jornal *The Guardian* onde relata que pelo menos trinta e cinco chefes de estado tiveram seus telefones celulares monitorados. A proposta de resolução destaca: "*deeply concerned at human rights violations and abuses that may result from the conduct of extra-territorial surveillance or interception of communications in foreign jurisdictions".*

O documento também destaca:

> "illegal surveillance of private communications and the indiscriminate interception of personal data of citizens constitutes a highly intrusive act that violates the rights to freedom of expression and privacy and threatens the foundation of a democratic society".

Dessa forma, Brasil e Alemanha buscam criar uma coalisão que, em conjunto com outras nações, possam garantir o sucesso da proposta de resolução como forma de reconhecer a privacidade como um direito internacional reconhecido.

Conforme destacado pela proposta de resolução: "*The General Assembly (...) affirms that the same rights that people have offline must also be protected online, in particular the right to privacy".* Ainda que este documento venha a sofrer alterações antes de ser adotado, o mesmo representa um passo para a garantia de que todas as

condições necessárias para prevenir estes tipos de violações sejam efetivamente cumpridas.

Este caso busca ilustrar a forma como governos mundiais podem literalmente ignorar os preceitos relacionados à privacidade. Todo o processo utilizado pela NSA norte-americana na espionagem de determinados governos e a vigilância de cidadãos revelam uma face bastante pertinente da forma como a segurança da informação e a privacidade devem ser tratados. A privacidade possui muitos significados, mas em vias gerais é a liberdade de não sofrer qualquer tipo de interferência ou intrusão; conforme citado por Louis Brandeis e Samuel Warren, o direito "de ser deixado só". Com isto, deve-se reconhecer e proteger a privacidade das pessoas em todos os níveis e esferas de interação social.

O episódio envolvendo os atos de vigilância e espionagem feitos pela NSA, conforme denunciado por Edward Snowden demonstram claramente a existência de interesses envolvidos. Atos de espionagem sempre existiram entre nações em toda a história humana. Para cada ato de espionagem existe outro de contra-espionagem, de forma que não há apenas uma única nação responsável por todo e qualquer ato dessa natureza. O que presenciamos agora é uma espécie de "guerra cibernética" onde todos os envolvidos necessariamente espionam e são espionados, numa batalha virtual onde vence quem possui e manipula efetivamente as informações obtidas.

A polêmica sobre a espionagem Norte-americana na Rede

O mundo da Internet presenciou nestes últimos tempos revelações surpreendentes, que mudaram todo comportamento dos usuários e governos ao redor do mundo no que diz respeito à Internet. Tudo teve início a partir das declarações públicas feitas por um ex-analista da NSA (*National Security Agency*), Edward Snowden, afirmando que o governo dos Estados Unidos monitora todo e qualquer comportamento dos usuários na Internet – não importando sua localização.

Todos estes segredos vieram a público graças à iniciativa de Snowden que durante entrevista declarou que "quem deve decidir se os governos devem – ou não – investigar o que as pessoas comuns fazem na Internet são os próprios cidadãos".

Sabe-se que atividades de espionagem e contra-espionagem são situações que acompanham os serviços de inteligência de todas as nações. Mas as declarações

fornecidas pelo ex-analista alcançaram um novo patamar: não só governos são vigiados ou espionados mas cidadãos comuns também o são.

As possibilidades de espionagem entre nações por meio da rede era algo especulável há um bom tempo, mas tudo isso se restringia somente à esfera de interesses políticos e estratégicos das nações.

As revelações feitas por Snowden trouxeram grande preocupação, fazendo com que surgisse à tona um assunto até então pertencente ao campo da estratégia para o campo da realidade. Uma realidade tão chocante quanto preocupante, pois agora o alvo são pessoas comuns que podem estar – e estão – sendo monitoradas e vigiadas em quase tudo o que é feito na rede mundial de computadores.

Portanto, o governo norte-americano por meio da NSA é responsável pelo monitoramento e vigilância de toda e qualquer pessoa no próprio território e no mundo, incluindo vários países. A iniciativa contou com a colaboração de grandes empresas de tecnologia, tais como Google, Microsoft, Apple, Facebook, LinkedIn e demais empresas pertencentes ao setor de telefonia.

A NSA, em termos gerais, cuida de assuntos relacionados à espionagem e serviços de inteligência. Nos Estados Unidos é o principal órgão responsável por toda a produção e gerenciamento de informações de inteligência (*Signals Intelligence – SIGINT*) para o governo.

Sua criação se deu anos após o fim da Segunda Guerra Mundial e alcançou grande atividade quando dos atentados às torres gêmeas em 11 de setembro de 2001. A partir de então os Estados Unidos tem tomado medidas bastante amplas no que diz respeito ao monitoramento, espionagem e contraespionagem, gerando um aporte de recursos humanos e financeiros bastante expressivos.

Em termos de recursos humanos e financeiros, a organização é tida como uma das maiores organizações de inteligência em solo americano, operando diretamente sob a jurisdição do Departamento de Defesa (*Department of Defense – DoD*) reportando-se diretamente ao diretor nacional de inteligência (*Director of National Intelligence*).

Nesse contexto, as principais funções da NSA estão diretamente ligadas à obtenção de informações, monitoramento, decodificação e análise das informações obtidas. As informações obtidas são utilizadas com o objetivo primário de espionagem e contraespionagem e pode-se incluir nesse contexto as atividades de monitoramento contra qualquer alvo determinado, independente de estar em solo americano ou em qualquer parte do mundo.

A NSA possui total autonomia para efetuar estes procedimentos, utilizando todo o aparato tecnológico disponível, inclusive contando com a colaboração de empresas de telefonia, haja visto que toda e qualquer chamada telefônica e conversações decorrentes destas chamadas são integralmente gravadas. Para compreender como a NSA conseguiu realizar estas e outras incursões pela rede, faz-se importante conhecer um pouco sobre o programa PRISM.

PRISM é um programa de monitoramento e obtenção de dados, desenvolvido e lançado em 2007 pela NSA, sendo um codinome para SIGAD US-984XN. No contexto da Internet, o PRISM armazena informações sobre buscas efetuadas através das empresas de tecnologia e Internet, tais como Google, Yahoo!, Apple, Facebook, Youtube, Microsoft etc.

Com tais recursos a NSA, por meio do PRISM faz um monitoramento constante e em tempo real de toda e qualquer atividade feita não só pela Internet – incluem-se aí os chats em redes sociais, e-mails, compras online ou navegação aleatória –, mas também através de chamadas telefônicas efetuadas. Com isto, toda e qualquer informação, não importando sua natureza ou mídia utilizada, encontra-se inteiramente nas mãos da NSA.

A importância e o papel das legislações nesse sentido revelam-se extremamente importantes para uma compreensão mais ampla do evento em destaque. O governo norte-americano fez valer o uso da própria legislação em vigor no país, o chamado "*USA Patriot Act*". Esta lei fora criada em 2001 com o objetivo de tornar as ações das agências de inteligência mais amplas e com maior foco na espionagem e obtenção de informações. A lei assegura que qualquer um que seja visto como uma ameaça à segurança nacional deve ser investigado.

Com este caso vimos que quando temos governos demostrando interesses em manipular, controlar ou censurar informações e recursos disponíveis na rede, toda a sociedade deve ser informada e mobilizada no sentido de coibir qualquer tentativa de apropriação de recursos ou informações de domínio particular. Um exemplo disso são as várias tentativas para aprovar o Marco Civil da Internet aqui no Brasil e da proposta de resolução da ONU sobre privacidade como um direito internacional; estas legislações surgem sempre com o pretexto de "defender os direitos e liberdades dos usuários". A sociedade deve buscar informações e tomar todas as providências cabíveis, para que não ocorra novamente uma repetição do "*USA Patriot Act*".

Técnicas e soluções para proteção online

Quando se fala em utilizar ferramentas e soluções para a proteção de sistemas no que se refere ao acesso à rede, podemos destacar o uso de normas, parâmetros e técnicas, conforme o nível de complexidade, usuários a serem atendidos e a natureza dos ativos de tecnologia envolvidos e a informação a ser protegida. Conforme ABNT ISO/IEC 17799:2005, todo e qualquer ativo deve ser protegido para que sejam garantidos os três princípios básicos de segurança da informação: Confidencialidade, Integridade e Disponibilidade.

Considerando a segurança da informação em ambiente corporativo ou ambientes de alto nível de complexidade, torna-se um tema de fundamental importância pois existe grande demanda por uma infraestrutura que possa tornar os processos de comunicação e transações o mais seguro possível. Para tais ambientes de alta complexidade, é altamente recomendável que se faça uso das normas ISO 17799 e ISO 27001, que dará o devido tratamento ao processo de implantação de técnicas e ferramentas de segurança da informação. Para o usuário comum, todas as ferramentas que visem a segurança da informação e respectiva proteção online podem ser utilizadas em maior ou menor grau; sua utilização dependerá da necessidade em cada situação ou cenário considerado.

A utilização de ferramentas e soluções para segurança da informação e proteção online, conforme destaca Cheswick (2005, p. 143-334) envolvem todo o conjunto de hardware, software e demais técnicas correlatas com o objetivo primordial de combater tentativas de ataque através da rede. Todas as ferramentas encontram-se disponíveis para diversas arquiteturas e plataformas de sistemas operacionais, podendo ser utilizadas de forma isolada ou combinada com outros recursos. Quanto ao seu tipo, as ferramentas podem ser classificadas conforme o escopo pretendido, conforme segue:

*** Ferramentas para Autenticação;**
*** Ferramentas para Segurança de Hosts;**
*** Ferramentas para Segurança de Redes;**
*** Ferramentas para Verificação de Vulnerabilidade e Integridade.**

Abaixo, apresentamos algumas das ferramentas mais utilizadas e demais mecanismos de segurança. Lembrando que os mesmos são utilizados tanto por empresas e instituições como também podem ser usados por usuários comuns. A decisão por utilizar um determinado programa ou tecnologia depende das especificações para cada uma das possibilidades existentes.

*** Política de Segurança:** Documento que define quais os direitos e responsabilidades que cada usuário possui em relação ao uso dos sistemas e recursos computacionais;

*** Notificação de incidentes:** Incidentes de segurança são eventos de caráter adverso, que podem ser confirmados ou estarem sob suspeita, no contexto da segurança de sistemas de informação ou redes de dados. A notificação deve ser feita sempre que houver atitudes que gerem certa desconfiança ou indiquem uma postura abusiva por parte dos usuários envolvidos. Notificações podem ajudar a proteger e contribui diretamente para a segurança global na Internet;

*** Criptografia:** Este recurso possibilita ao usuário proteger seus dados e informações contra acessos indevidos, independente de trafegarem pela rede ou estarem gravados no próprio computador ou dispositivo;

*** *Backup* (cópia de segurança):** Recurso utilizado para geração de cópias de segurança de qualquer dado ou informação existente em computadores e demais dispositivos correlatos. Possibilita a proteção das informações e sua respectiva recuperação em caso de falha do sistema operacional, roubo ou destruição das informações;

*** Logs de eventos (*Logs*):** Registro de toda e qualquer atividade de usuários de sistemas e demais programas em operação num determinado momento. Tais registros normalmente ficam armazenados em bases de dados ou em arquivos no próprio computador. *Logs* são extremamente úteis no processo de auditoria de sistemas, onde são verificadas todas as atividades e aplicações executadas e o tempo de utilização do sistema;

*** *Antimalware*:** Ferramentas que possibilitam uma varredura específica nos sistemas, buscando detectar e anular os efeitos ocasionados por códigos maliciosos presentes num determinado dispositivo. Enquadram-se nessa categoria programas como antivírus, antitrojan, antispyware, antirootkit entre outros;

*** Filtros *Antispam:*** Recurso que permite fazer uma filtragem dos *e-mails* recebidos, permitindo separar os e-mails desejados dos indesejados. A maioria dos leitores de e-mail e *webmails* atuais possuem essa funcionalidade;

*** Firewall:** Programa ou dispositivo de hardware que controla o fluxo de dados de entrada e saída de informações, analisando o tipo de pacote de dados e determinando se o mesmo possui ou não autorização para acessar determinadas estações e/ou aplicações. Baseia-se na utilização e aplicação de regras existentes nesses dispositivos ou programas;

*** *Intrusion Detection System* (*IDS*):** São conhecidos como Sistemas de Detecção de Intrusos. Estes softwares funcionam em conjunto com sistemas de *firewall* proporcionando maior segurança durante o processo de comunicação de dados.

Este caso procurou abordar os principais recursos e sua vital importância para a segurança de sistemas em redes de dados, de forma a proporcionar o uso seguro e efetivos de todos os recursos disponibilizados pela Internet.

Para cada tipo de cenário considerado, sejam ambientes corporativos ou institucionais, deve-se avaliar adequadamente quais ferramentas e recursos são necessários a cada tipo de ambiente e quais as demandas de cada setor ou departamento e usuários envolvidos, de forma a determinar quais os potenciais riscos existentes e a forma adequada de mitigá-los.

Para usuários comuns, em ambiente de redes domésticas, pode-se abordar o tema de forma mais simples. O uso de *softwares* como antivírus, *antispyware*, *firewall* aliados a um sistema operacional atualizado podem fazer a diferença para uma maior segurança e privacidade na rede. Deve-se também dar grande ênfase nos métodos e nas recomendações para uma navegação segura na Internet.

5 CONCLUSÃO

Uma abordagem que concentre o foco na segurança da informação e na privacidade na rede nos dias atuais pode ser bastante complexa, dado ao alto nível de desenvolvimento das tecnologias de rede correlatas e o caráter cada vez mais dinâmico e social proporcionado pela interação entre usuários e tecnologias.

A oferta de soluções para mitigar os riscos decorrentes da manipulação de dados e informações e toda a interação com os recursos oferecidos em rede atraem um número cada vez maior de usuários; grandes corporações e instituições são de longe os maiores interessados. Independente do ramo de negócios ou serviços oferecidos, torna necessário a plena garantia de quesitos como confidencialidade, integridade e disponibilidade.

O desenvolvimento das tecnologias da informação em conjunto com a evolução das tecnologias relacionadas às redes de dados trouxeram um horizonte sem limites. Miríades de possibilidades passam a estar ao alcance de apenas toques no teclado ou cliques do *mouse.*

Oportunidades de negócio, aprendizado, ampliação das redes de contatos e relacionamentos ou mesmo a pura e simples navegação pela Internet passou a ser algo tão arraigado nesta sociedade quanto qualquer outra atividade humana. Em decorrência desse fato, um mundo passou a estar ao alcance de nossas mãos e de nossa imaginação. Uma evolução sem precedentes na história humana, com uma demanda crescente em torno da oferta e procura de produtos, serviços, entretenimento e conhecimento.

“Conhecimento é poder”, como bem disse Francis Bacon. E a necessidade de conhecimento tem se mostrado cada vez mais evidente em nossa sociedade. A chamada sociedade do conhecimento está cada vez mais em busca de novas formas de conhecimento e principalmente de métodos e técnicas para a sua aplicação. A produção de todo esse conhecimento decorre necessariamente da organização e sistematização de dados em informação.

Com tantos dados e informações transitando a cada segundo pela rede, é evidente o interesse em garantir que tais dados e informações possam ter sua plena garantia de que estarão seguros e disponíveis, sejam eles particulares ou públicos.

Com todas as inúmeras possibilidades de uso e manipulação de dados e respectivo processamento surgiram também grandes problemas e questões altamente complexas. Trata-se não apenas de um mero “mundo virtual” onde praticamente tudo pode apresentar-se virtualmente acessível e compartilhável; deve-se considerar que estamos manipulando informações sobre entidades e pessoas que realmente se fazem presentes no mundo virtual, mas que também encontram-se fora dele – o mundo real. Estas considerações nos levam a ponderar que para quaisquer atividades realizadas na Internet e a utilização efetiva de todos os recursos por ela oferecidos, devem ser feitos de forma responsável e ética.

6 REFERÊNCIAS

STEFANICK. Lorna. Controling Knowledge – Freedom of Information and Privacy Protection in a Networked World. AU Press. 2011.

NORMA BRASILEIRA ABNT NBR ISO/IEC 17799:2005. Tecnologia da Informação – Técnicas de Segurança – Código de prática para gestão da Segurança da Informação.

KLEINIG, John. et al. Security and Privacy – Global Standards for Ethical Identity Management in Contemporary Liberal Democratic States. Washington: Brookings, 1997.

MUNGO, Paul. GLOUGH, Bryan. Approaching Zero – The Extraordinary World of Hackers, Phreakers, Virus Writers and Keyboard Criminals. Random House. 1992.

ALCALÁ, Humberto Nogueira. Autodeterminación informativa y hábeas data em Chile e información comparativa. In: Anuário de Derecho Constitucional Latioamericano 2005, Tomo II, Konrad Adenauer Stiftung, p. 449.

PÉREZ LUÑO, Antonio-Enrique. Manual de Informática e Derecho. Barcelona: Editorial Ariel, 1996, p. 43.

OPEN SECURITY FOUNDATION. Data Loss statistics. In: DataLossdb. 2013. Disponível em: <http://datalossdb.org/statistics>. Acesso em: 5 jun. 2013

PRIVACY RIGHTS CLEARINGHOUSE. Chronology of Data Breaches: Security Breaches 2005- Present. [USA], 2013. Disponível em: <http://www.privacyrights.org/data-breach>. Acesso em: 9 maio 2013.

Fred H. Cate. Privacy in the information age. Washington: Brookings, 1997.

REINALDO FILHO, Demócrito (coord.). Direito da Informática – temas polêmicos. 1a Ed., Bauru, SP: Edipro, 2002.

COSTA JUNIOR., P. J. da. O direito de estar só: tutela penal da intimidade. 4. ed. São Paulo: Revista dos Tribunais, 2007.

David Heald. Varieties of Transparency. Proceedings of the British Academy, 135, 25-43. The British Academy 2006.

BENNETT, Colin. Regulating Privacy: data protection and public policy in Europe and the United States. Op. Cit., p. 43.

DE LA CUEVA, Pablo Lucas Murillo. La construcción del derecho a la autodeterminación informativa. In: Revista de Estudios Políticos ,104 (Nueva Época), Abril/Junio 1999, Madri, p. 38

LIMA, Caio Cesar Carvalho. MONTEIRO, Renato Leite. Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada. Disponível em:<http://www.atoz.ufpr.br/index.php/atoz/article/view/41>. Data de acesso: 03 de fevereiro de 2014.

CASTELLS, Manuel. A era da informação: economia, sociedade e cultura. Vol 1. A sociedade em rede. Trad: Roneide Venâncio Majer. São Paulo: Paz e Terra, 1999, p. 50.

O CGI.br e o Marco Civil da Internet. Disponível em: <http://www.cgi.br/publicacoes/documentacao/CGI-e-o-Marco-Civil.pdf> Data de acesso: 08 de janeiro de 2014.

UN News Centre. Disponível em: <http://www.un.org/apps/news/story.asp?NewsID=46780&Cr=privacy&Cr1=#.UwH8NXVdURg> Data de acesso: 17 de fevereiro de 2014.

Center for Democracy & Technology – Keeping the Internet Open-Innovative-Free. Disponível em: <https://www.cdt.org/content/nsa-surveillance>

CHESWICK, W.; BELLOVIN, S. M.; RUBIN, A. D.; Firewalls e Segurança na Internet. 2.ed. RS. Bokman. 2005.