UM DEBATE SOBRE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE À LUZ DO MARCO CIVIL DA…

Conference Paper · January 2016

CITATIONS
0

READS
2

4 authors, including:

Nathalia Patrício
University of São Paulo
13 PUBLICATIONS **6** CITATIONS
SEE PROFILE

Edison Spina
University of São Paulo
37 PUBLICATIONS **8** CITATIONS
SEE PROFILE

UM DEBATE SOBRE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE À LUZ DO MARCO CIVIL DA INTERNET[1]

Nathalia Sautchuk Patrício[2]; Vera K. S. Kerr[3]; Davi Kerr[4]; Edison Spina[5]

Resumo: Este artigo pretende estabelecer um paralelo entre a área de segurança da informação e o Marco Civil da Internet. Além disso, pretende explorar algumas das práticas atualmente utilizadas no contexto da Internet, a fim de garantir o que está estabelecido na lei, em especial no tocante à privacidade dos usuários e à proteção dos dados pessoais.

Palavras-chave: Segurança da informação, privacidade, Marco Civil da Internet; criptografia, spam, DDoS.

Abstract: This article aims to establish a parallel between the Marco Civil da Internet and Information Security area. In addition, it intends to explore some of the practices currently used in Internet context in order to ensure what is established in the law, especially with regard to users privacy and personal data protection.

Keywords: Information security, privacy, Marco Civil da Internet; cryptography, spam, DDoS.

1. INTRODUÇÃO

Dentro da área de segurança da informação diz-se que um sistema seguro é aquele que fornece informações íntegras somente a usuários autorizados, no momento em que elas são pedidas através de requisições válidas e identificadas, não permitindo que essas informações sejam recebidas, observadas ou alteradas por terceiros não autorizados (STALLINGS E BROWN, 2011). Há diferentes aspectos que caracterizam a segurança de um sistema de computadores, conhecidos como serviços de segurança. Dentre os serviços básicos de segurança está a confidencialidade de dados, que é a garantia de que qualquer informação armazenada num sistema de computação ou transmitida via rede seja revelada, acessada e manipulada somente por usuários devidamente autorizados. A confidencialidade tem relação com a privacidade, sendo que esta última pode ser definida como a garantia de que os indivíduos controlam ou influenciam quais informações sobre eles podem ser coletadas e armazenadas e por quem e para quem tais informações podem ser reveladas

---

1 . Artigo apresentado ao Eixo Temático 14 – Privacidade / Vigilância / Controle do IX Simpósio Nacional da ABCiber.

2 Pesquisadora é engenheira de computação e doutoranda em Engenharia da Computação na Escola Politécnica da USP. E-mail: nathysautchuk@usp.br

3 Pesquisadora é advogada e doutoranda em Engenharia da Computação na Escola Politécnica da USP. E-mail: verakerr.br@gmail.com

4 Pesquisador é mestrando em Engenharia da Computação na Escola Politécnica da USP. E-mail: davikerr.br@gmail.com

5 Pesquisador é professor do Departamento de Engenharia da Computação e Sistemas Digitais da Escola Politécnica da USP. E-mail: spina@usp.br

(STALLINGS E BROWN, 2011). Porém, a privacidade, além de abranger a confidencialidade de dados, também envolve as políticas de uso por usuários autorizados.

Sob a ótica do direito há um consenso tanto do ponto de vista doutrinário bem como jurisprudencial quanto à necessidade da tutela da privacidade de forma mais ampla possível, visto ser a mesma direito da personalidade, considerado direito fundamental tendo como suporte o princípio da dignidade humana, consagrado no texto constitucional de 1988. O conceito amplo de privacidade engloba a ideia de controle sobre informações e dados pessoais. Portanto, a privacidade, sob essa ótica, seria o direito de pessoas, grupos ou instituições deter o controle de quando, de que forma e sob que extensão informações sobre si seriam reveladas a terceiros segundo Leonardi (2012).

No Brasil, a Lei nº 12.965, conhecida como Marco Civil da Internet, está em vigor desde 2014 e coloca a proteção da privacidade e a proteção dos dados pessoais como fundamentos que disciplinam o uso da Internet no Brasil (BRASIL, 2014, Art. 3º, II, III).

De acordo com a mesma lei (BRASIL, 2014, Art. 7º), o acesso à internet é essencial ao exercício da cidadania e 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 (BRASIL, 2014, Art 8º). Tendo isso em vista, são assegurados diversos direitos aos usuários, sendo que dentre esses estão a inviolabilidade da intimidade, da vida privada e das comunicações privadas pela Internet e aquelas já armazenadas (salvo por ordem judicial); o não fornecimento a terceiros dos dados pessoais (salvo mediante consentimento livre, expresso e informado); informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção dos dados pessoais, que somente poderão ser utilizados para finalidades que justifiquem sua coleta, que não sejam vedadas pela legislação e que estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de Internet mediante consentimento expresso; e exclusão definitiva dos dados pessoais que tiverem sido fornecidos a determinada aplicação de Internet, ao término da relação entre as partes.

Apesar de todos esses direitos ao usuário em relação à sua privacidade e a proteção de seus dados na Internet estarem assegurados, até o início do ano de 2016, ainda estava em aberto como esses direitos poderiam ser garantidos na prática. O decreto nº 8.771 veio elucidar alguns pontos no que concerne aos padrões de segurança e sigilo dos registros, dados pessoais e comunicações privadas. Segundo esse decreto (BRASIL, 2016, Art. 13), os provedores de conexão e de aplicações devem estabelecer controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários; devem prever mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros; devem criar inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado; e devem usar soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

No entanto, como essa regulamentação é recente, permanecem dúvidas se as medidas previstas no decreto serão suficientes para assegurar a privacidade dos usuários. Ainda não há nenhum estudo substancial que relacione a área de segurança da informação e o Marco Civil da Internet. Um dos debates importantes a serem feitos é sobre como boas práticas existentes nessa área poderiam ser aplicadas na garantia da privacidade e na proteção dos dados pessoais dos usuários da Internet assegurada através dessa lei e seu decreto regulamentador.

Primeiramente, serão explorados alguns aspectos do Marco Civil da Internet e do seu decreto regulamentador. Depois, serão apresentados alguns conceitos de segurança da informação. O item IV faz um comparativo entre o modelo de segurança da informação e o Marco Civil da Internet. Os itens seguintes apresentam três casos: o controle de spam no Brasil, o uso da criptografia e suas controvérsias e o combate do ataque conhecido como DDoS. Para finalizar são apresentadas algumas considerações finais do trabalho.

2. MARCO CIVIL DA INTERNET

De acordo com Solagna (2015) a proposta do Marco Civil da Internet nasceu como uma reação à tendência criminalizante no tratamento de diversos comportamentos na Internet e na Web que se apresentava no projeto de lei 89/2003. Esse projeto de lei, que era um agregado de outras iniciativas legislativas com o objetivo de modificar o código penal para tipificar "crimes cibernéticos", gerou um projeto substitutivo de autoria do deputado Eduardo Azeredo que foi reapresentado em 2006.

Ao contrário da prática legislativa tradicional, o Marco Civil não foi uma proposta de governo ou do próprio legislativo, mas uma proposta da sociedade por meio de uma plataforma colaborativa totalmente inovadora valendo-se da própria estrutura da Internet. Desde o início, a proposta da lei se baseou em diversos fundamentos, tais como a liberdade de expressão, os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais, a pluralidade e a diversidade, a abertura e a colaboração, a livre iniciativa, a livre concorrência e a defesa do consumidor e a finalidade social da rede (BRASIL, 2014).

Vários princípios que disciplinam o uso da Internet também foram reconhecidos na lei, dentre os quais destacam-se a proteção da privacidade, proteção dos dados pessoais, e a preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas (BRASIL, 2014). Esses princípios têm relação direta com a área de segurança da informação, uma vez que as práticas dessa área podem ajudar a promovê-los.

Além dos princípios anteriormente mencionados, o Marco Civil da Internet também apresenta um rol de garantias, direitos e deveres dos internautas sendo estruturado a partir de três pilares: neutralidade de rede, liberdade de expressão e privacidade. Introduz o tema da proteção de dados pessoais no sistema jurídico brasileiro no âmbito do espaço virtual a partir da perspectiva de que as pessoas são titulares de seus dados, prescreve regras sobre o consentimento para tratamento de dados, autoriza a coleta de dados apenas quando relacionados com a finalidade da atividade prestada, reitera a necessidade de transparência nas políticas de privacidade, entre outras. Trata-se de diploma legal que consagra um conjunto de princípios a partir dos quais fundam-se as relações jurídicas no âmbito da tecnologia no país, razão pela qual o Marco Civil foi "batizado" pela expressão "Constituição da Internet", visto que dispõe sobre as bases à luz das quais devem ser interpretadas as normas integrantes do nosso sistema jurídico quando relacionadas à Internet, incluindo as tecnologias da informação e comunicação em geral (LEMOS, 2014).

Ao mesmo tempo que consagra princípios fundamentais do texto constitucional no ambiente virtual, o Marco Civil da Internet também legitima os direitos civis no ambiente da Rede. Ao invés de ser um diploma legal repressivo tipificando condutas ilícitas, estabeleceu-se como fundamento de direitos e garantias civis, promovendo segurança jurídica na medida que estabelece um padrão legal às decisões judiciais.

No tocante à tutela da privacidade no Brasil, até a edição da referida lei, o acesso a dados e condutas dos usuários na Internet era praticamente isento de regulação, sujeitando o internauta a frequentes abusos.

Informações sobre sua navegação na rede, tais como quais sites acessou, quando, por quanto tempo e até mesmo o conteúdo de e-mails eram possíveis de serem obtidos por autoridades públicas sem autorização judicial, sendo muitas vezes consideradas válidas como prova em processo administrativo e judicial. Em função desses abusos, o Marco Civil inovou ao preconizar que nenhum dado do usuário pode ser acessado sem ordem judicial prévia que autorize esse acesso, estabelecendo inclusive critérios para tanto (LEMOS, 2014).

Buscou-se, portanto, impedir que, atraídos pela oportunidade de ganho que o armazenamento e o acúmulo de dados pessoais possibilita, prestadores de serviço desviem-se da atividade para a qual foram contratados, utilizando-se dos referidos dados em proveito próprio, considerando a possibilidade de controle e monitoramento que o ambiente da Internet proporciona. Dessa forma, o Marco Civil da Internet tutela a privacidade na medida que define limites de atuação aos diferentes *players*, impedindo o acúmulo de dados estranhos à transação e estabelecendo relação de transparência ao permitir que o usuário saiba quais dados seus serão armazenados se aceitar os termos de serviço de um provedor, entre outros.

O Brasil ainda não tem legislação específica sobre proteção de dados pessoais, apesar de haver disposições gerais que tratem da matéria previstas na Constituição Federal, no Código Civil, no Código de Defesa do Consumidor, na Lei de Interceptação Telefônica (Lei nº 9.296/96), na Lei Geral de Telecomunicações (Lei nº 9.472/1997), entre outras, inclusive no próprio Marco Civil da Internet conforme já mencionado. Contudo, esta lacuna legal ainda não foi suprida, deixando o usuário em posição vulnerável em face do Estado e de organizações cujas práticas sejam violadores da privacidade. Atualmente, este tema é objeto de projeto de lei que está sendo discutido no Congresso Nacional fortemente inspirado na legislação europeia (LEITE, 2014).

Por fim, resta esclarecer que o Marco Civil buscou garantir aos internautas segurança na navegação, sem que isso signifique que o regramento por ele veiculado sobre a privacidade e proteção de dados pessoais seja suficiente e capaz de prescindir de legislação específica.

3. SEGURANÇA DA INFORMAÇÃO

A segurança da informação é um processo da organização, que deve considerar a informação tanto no ambiente convencional quanto no ambiente de tecnologia. A utilização da informação acontece pelas pessoas e a segurança também deve acontecer pelas pessoas. Segundo Fontes (2012) uma definição mais formal para segurança da informação seria o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada.

Um modelo que ajuda a entender a área é o Cubo de McCumber como pode ser visto na figura 1. Nele cada um dos eixos especifica uma característica da segurança da informação (MCCUMBER, 1991). Um dos eixos trás os objetivos dos sistemas de segurança, que são a confidencialidade (que engloba a privacidade), a integridade e a disponibilidade. No outro eixo, há os estados da informação, sendo eles a transmissão, o armazenamento e o processamento. O último eixo é o do salvaguardas, que são a tecnologia, as políticas e práticas e os fatores humanos.

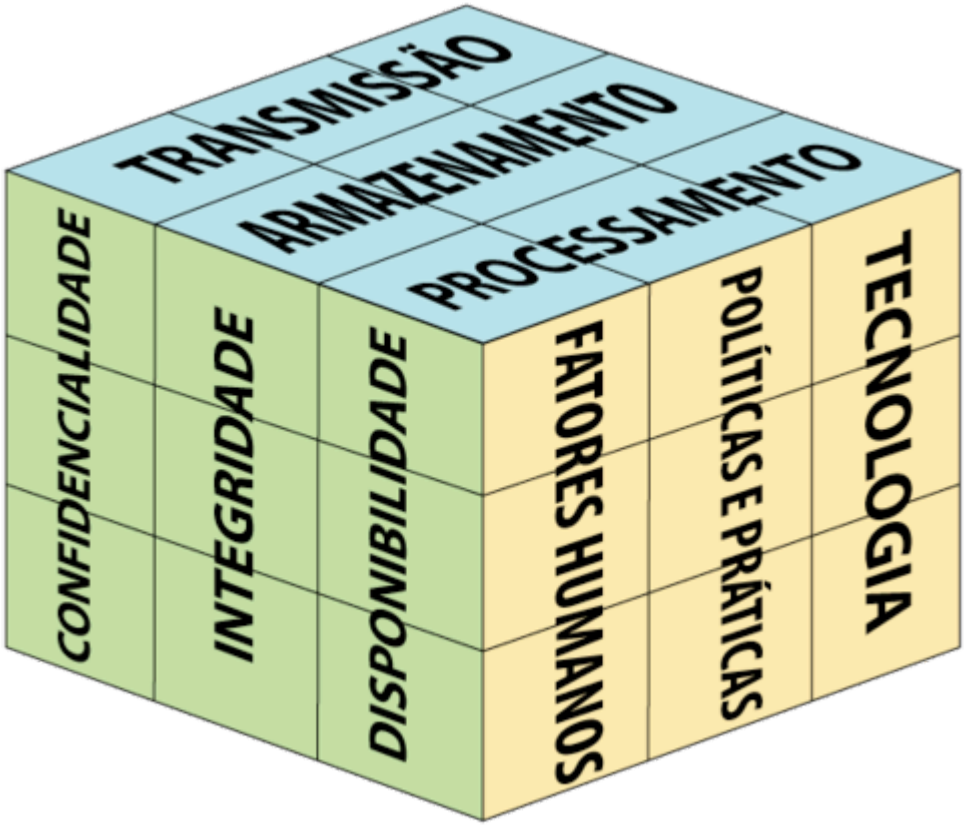

Figura 1: Cubo de McCumber (INSTITUTO OPERREDE, s.d.)

Esse modelo pode ser usado para pensar em ações voltadas a garantia de alguns dos direitos dos usuários na Internet de acordo com o Marco Civil da Internet.

4. SEGURANÇA DA INFORMAÇÃO E O MARCO CIVIL DA INTERNET

O modelo de McCumber pode ser útil para compreender como certos artigos do Marco Civil da Internet se relacionam com a área de segurança da informação e, com isso, vislumbrar formas de garantir a sua efetividade na prática.

Fazendo um comparativo dos objetivos dos sistemas de segurança da informação com a lei, pode-se identificar dois artigos (3º e 8º) em que a privacidade é colocada como algo a ser garantido na Internet. Sendo assim, os salvaguardas a serem implementados devem levar em consideração esse objetivo.

O Marco Civil da Internet estabelece a privacidade e a proteção de dados pessoais como princípios fundamentais do internauta conforme anteriormente exposto, segundo prevê seu artigo 3º, inciso II e III. Preceitua ainda ser direito e garantia dos usuários a exigência de sua concordância que deve ser livre, expressa e justificada, para que ocorra a coleta, o uso, o tratamento e o armazenamento dessas informações, em consonância com o estabelecido no artigo 7º, VIII e IX.

Por outro lado, o artigo 8º disciplina que "a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet" e por isso, determina, em

seu parágrafo único, a nulidade de pleno direito das cláusulas que, conforme o inciso I, desrespeitem à inviolabilidade e o sigilo de comunicações particulares, veiculadas pela internet (LEITE, 2014).

No caso dos estados da informação do modelo de McCumber, pode-se fazer um paralelo entre os estados de transmissão e armazenamento e o artigo 7º da lei (BRASIL, 2014, Art 7º). Nele é mostrada a preocupação da garantia da inviolabilidade do fluxo das comunicações pela Internet e do sigilo das comunicações privadas armazenadas.

A preocupação com os salvaguardas da segurança da informação também aparece algumas vezes na redação da lei, especificamente em relação a adoção de políticas claras por parte das empresas prestadoras de serviços de conexão à Internet. No artigo 7º, os usuários devem ter asseguradas informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de Internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade. A questão da coleta de dados pessoais e seu fornecimento a terceiros também deve ser informada claramente e os usuários devem consentir com os termos mediante consentimento livre, expresso e informado.

O artigo 7º deve ser interpretado sob dois aspectos: numa primeira perspectiva estão assegurados os direitos da privacidade e intimidade do usuário que recebem salvaguarda constitucional e são as prerrogativas do indivíduo considerando sua inserção num estado democrático de direito; já sob uma segunda perspectiva, entende-se que esses direitos permanecem preservados quando inseridos num banco de dados ou durante seu tráfego pela rede, ou seja, a proteção objetiva conferida pelo Marco Civil aos dados pessoais é, por reflexo, a mesma proteção conferida pela lei ao titular dos dados.

Segundo o artigo 7º, VIII e IX há regramento quanto à coleta executada pelos provedores. Inicialmente, é estabelecido que apenas podem ser extraídos dados para os quais haja motivo justificável para a sua captação, condicionada à ausência de impedimento legal para a sua realização, sendo indispensável que estejam diretamente discriminados nos termos de uso ou em contratos. Passou a ser imperativo, portanto, a elaboração de documento, alertando os internautas a respeito dos procedimentos de captação, uso, tratamento e armazenamento de dados, determinando-se com transparência e clareza de quais dados serão coletados, zelando os provedores pela lisura de seus atos (Paesani, 2014)

A questão tecnológica dos salvaguardas aparece claramente no decreto regulamentador. O artigo 13 fala explicitamente que os provedores de conexão e de aplicações devem observar algumas diretrizes sobre padrões de segurança, como controle de acesso aos dados de usuários com uso de mecanismos de autenticação, inventário dos acessos aos dados e a garantia da inviolabilidade dos dados através de uso de soluções como encriptação (BRASIL, 2016, Art. 13). De acordo com Tanembaum e Wetherall (2011), com exceção da segurança na camada física, quase toda a segurança se baseia em princípios criptográficos. Portanto, uma das discussões mais importantes é sobre seu uso de acordo com o Marco Civil da Internet como uma das formas de garantir a eficácia da lei.

O decreto também estabelece que "cabe ao CGI.br promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais" para captação, armazenamento e tratamento de dados pessoais e comunicações privadas (art. 13). Isso não significa que o Comitê Gestor da Internet no Brasil (CGI.br) substitui a Autoridade de Proteção de Dados Pessoais, sendo que o Congresso Nacional tem competência para definir

regramento específico mediante aprovação de lei específica que discipline os direitos dos usuários e os deveres das empresas envolvidas na captação e processamento desses dados.

O decreto regulamentador prevê ainda a definição de dado pessoal e estabelece que as empresas trabalham com dados pessoais de usuários, devem mantê-los em "formato interoperável e estruturado" para viabilizar o acesso resultante de mandado judicial. Estabelece ainda que, após finalizada a razão pela qual o dado pessoal foi captado e o registro de conexão, o provedor deve excluir os referidos dados (art. 13, § 2º).

Nos itens a seguir serão apresentados três casos em que algumas técnicas e tecnologias podem ser usadas para assegurar a segurança da informação na Internet.

5. CONTROLE DE SPAM NO BRASIL

Uma boa prática de segurança da informação no ambiente da Internet é a diminuição do envio de mensagens de correio eletrônico não autorizadas, comumente conhecidas como spam. Apesar desse tipo de mensagem ser utilizada para propaganda de produtos e serviços legítimos, na maioria dos casos é usado para disseminar programas maliciosos com o intuito de violar a privacidade dos usuários da Internet. Segundo Hoepers et al. (2015), no ano de 2009, o Brasil foi o primeiro colocado no ranking da Composite Blocking List dos países que mais enviavam spam, sendo classificado como "Rei do Spam" pela mídia internacional. Devido a essa má fama, chegou-se a casos extremos de blocos inteiros de IPs brasileiros serem bloqueados no tráfego de entrada de outros países, por critério apenas de nacionalidade.

Caio Miachon Tenório, comentando decisão judicial relacionada a envio de spam cita o autor Flávio Tartuce que entende que "o spam configura flagrante abuso de direito, assemelhado ao ato ilícito pelas eventuais consequências, contraria o fim social e econômico da grande rede, o que já serviria para enquadrar a prática como abuso de direito, como conduta atentatória à boa-fé objetiva (TARTUCE, Flávio. Manual de Direito Civil. São Paulo: Método, 2011, p. 449-450)".

O referido autor menciona ainda que Tarcísio Teixeira, por sua vez, "vai além, aplicando responsabilidade civil objetiva até mesmo para o provedor de e-mails, atribuindo-lhe o dever de indenizar o consumidor lesado pelo recebimento do spam. Para esse autor, se é o provedor quem faz a mensagem indesejada chegar ao usuário, nos termos do artigo 3º, caput do Código de Defesa do Consumidor, ele passa a ser fornecedor, por tal razão, cabe a ele também a responsabilidade pela reparação do dano causado (TEIXEIRA, Tarcísio. Curso de Direito e Processo Eletrônico. São Paulo: Saraiva, 2013, p. 204)".

Como medida de mitigação desse problema foi adotada uma boa prática chamada de gerência da porta 25. A porta 25 é a porta padrão do protocolo TCP/IP utilizada para envios de correios eletrônicos entre servidores de e-mail que se utilizam do protocolo SMTP (HOEPERS ET AL, 2015). Uma porta nada mais é do que conexão lógica para transmissão de dados entre dispositivos na rede. Quando um usuário submete um e-mail na Internet, a mensagem vai para um servidor de e-mail e este servidor usa a porta 25 para entregá-la para o servidor de destino. A questão é que essa porta não necessita de autenticação para ser usada e assim os programas maliciosos podem se passar por servidores de e-mail, conforme funcionamento ilustrado na figura 2. Com isso, as máquinas infectadas de usuários brasileiros eram usadas, sem seu conhecimento, para encaminhar spam vindo de remetentes estrangeiros em quantidade massiva para usuários em todo o mundo, de forma não identificável (HOEPERS ET AL, 2015).

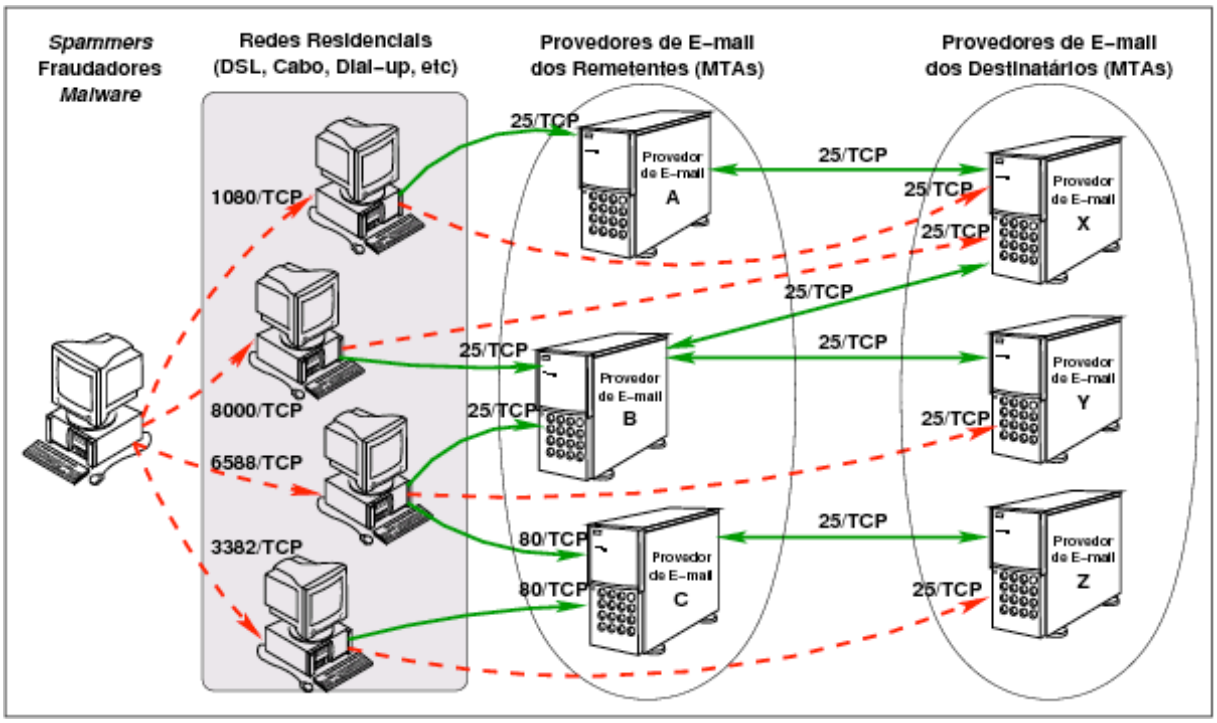

Figura 2: Cenário de abuso da porta 25 (Antispam.br, s.d.)

A partir da implementação da gerência da porta 25, o usuário residencial passou a poder somente enviar correio eletrônico para um servidor de e-mails e não diretamente para outros usuários. Em suma, a submissão de e-mail ficou bloqueada na porta 25 para usuários residenciais, passando a ser desempenhada por uma porta exclusiva para esse fim (porta 587), que exige autenticação com senha, como mostrado na Figura 3. Essa medida é uma prática incentivada pela IETF (Internet Engineering Task Force), organização internacional responsável pela elaboração de padrões de diversos aspectos de funcionamento da rede, através da BCP 134 (Best Current Practice). No Brasil, o CGI.br teve um papel importante no incentivo à adoção dessa prática pelas empresas de provimento de conexão à Internet que foi tida como exitosa no combate ao spam (HOEPERS ET AL, 2015).

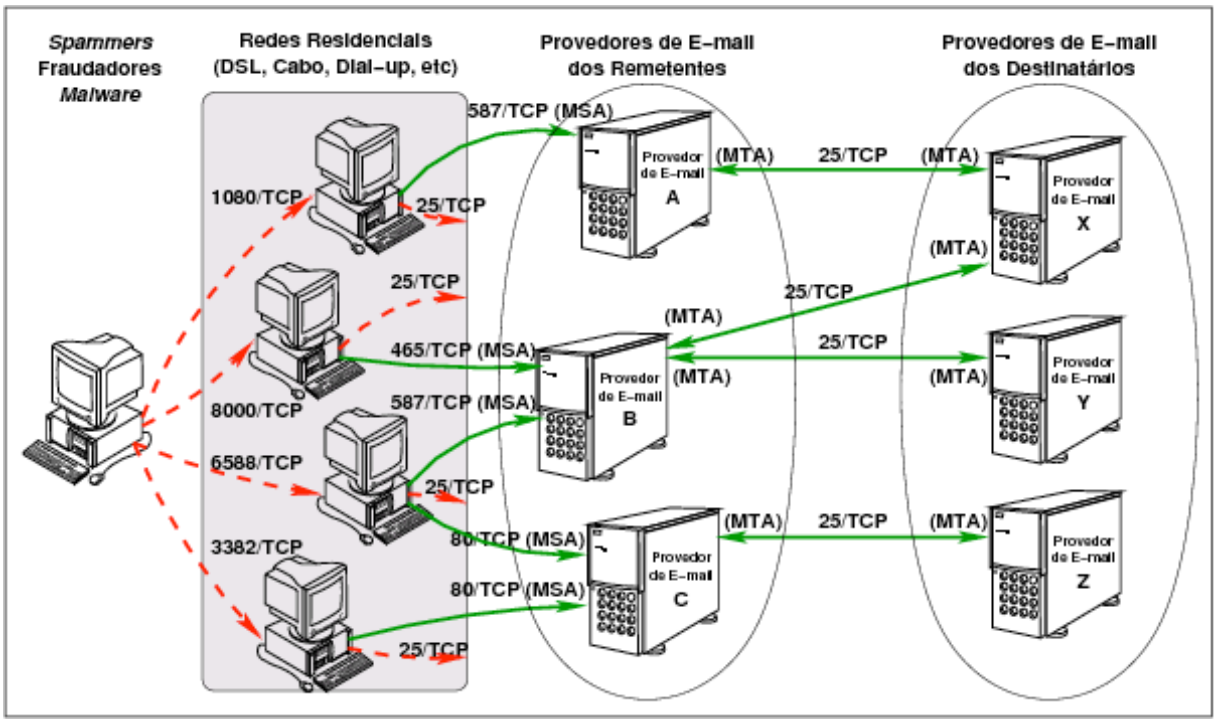

Figura 3: Cenário após a adoção da gerência da porta 25 (Antispam.br, s.d.)

6. A CONTROVÉRSIA NO USO DA CRIPTOGRAFIA

Outra boa prática de segurança da informação é o uso de criptografia para a transmissão de dados através da Internet e no armazenamento deles em servidores na rede. A criptografia ajuda a garantir a confidencialidade dos dados e, em certa medida, a privacidade dos usuários (STALLINGS E BROWN, 2011).

Além disso, a criptografia é um mecanismo eficaz de combate a espionagem promovida pelos governos. Os governos não apreciam essa possibilidade de uma privacidade real, através da qual é muito mais difícil seus agentes espionarem criminosos de todos os tipos, mas também é muito mais difícil fazer o mesmo com jornalistas e adversários políticos (TANEMBAUM E WETHERALL, 2011).

De forma resumida, Tanembaum e Wetherall (2011) dizem que as mensagens a serem criptografadas, conhecidas como texto simples, são transformadas por meio de uma função parametrizada por uma chave. Em seguida, a saída do processo de criptografia, conhecido como texto cifrado, é transmitida. Stallings (2015) define o processo de converter um texto claro em um texto cifrado como cifração ou encriptação, enquanto que restaurar o texto claro a partir do texto cifrado é a decifração ou decriptação.

Em um caso recente no Brasil, o aplicativo WhatsApp teve seu funcionamento suspenso no país devido ao descumprimento de ordem judicial de fornecimento de dados à Justiça. A empresa diz não poder fornecer os dados requeridos devido a utilização da criptografia ponta a ponta. Segundo Alves (2016), a juíza exigiu "a desabilitação da chave de criptografia", alegando, inclusive, não ser possível a prestação de serviços de comunicação digital no mercado brasileiro que impeçam a efetividade da Justiça criminal. Esse caso trouxe à tona um debate sobre a legalidade do uso da criptografia no Brasil. Por um lado, o próprio decreto regulamentador do Marco Civil da Internet coloca a criptografia como uma das técnicas a serem utilizadas para garantir a inviolabilidade dos dados, por outro, com base na mesma lei, uma juíza questiona seu uso, citando-na como impeditivo para o cumprimento das medidas judiciais necessárias.

Ainda em relação à decisão judicial acima mencionada cumpre registrar interessante comentário elaborado por Veridiana Alimonti em que ela afirma que: "a insegurança nas comunicações e o comprometimento do direito à privacidade prejudicam a liberdade de expressão. Justamente por isso a criptografia já foi defendida por diferentes Relatores Especiais para a Liberdade de Expressão da ONU (Frank La Rue e David Kaye) em seus documentos. Em relatório divulgado em 2015, David Kaye recomenda que Estados não restrinjam a criptografia, que facilita e contribui ao exercício da liberdade de opinião e expressão. Assim, proibições genéricas a esse recurso não são necessárias nem proporcionais. Ao mesmo tempo, os Estados devem evitar quaisquer medidas que enfraqueçam a segurança dos indivíduos online, tais como backdoors, padrões fracos de criptografia, entre outros (A/HRC/29/32, pg. 20, item 60)".

Devido a essa controvérsia, o STF convocou uma audiência pública para tratar a questão da criptografia do WhatsApp e colocou as seguintes questões para serem respondidas por especialistas:

> 1 – Em que consiste a criptografia ponta a ponta (end to end) utilizada por aplicativos de troca de mensagens como o WhatsApp?
>
> 2 – Seria possível a interceptação de conversas e mensagens realizadas por meio do aplicativo WhatsApp ainda que esteja ativada a criptografia ponta a ponta (end to end)?
>
> 3 – Seria possível desabilitar a criptografia ponta a ponta (end to end) de um ou mais usuários específicos para que, dessa forma, se possa operar interceptação juridicamente legítima?
>
> 4 – Tendo em vista que a utilização do aplicativo WhatsApp não se limita a apenas uma plataforma (aparelhos celulares/smartphones), mas permite acesso e utilização também em outros meios, como, por exemplo, computadores (no caso do WhatsApp mediante o WhatsApp Web/Desktop), ainda que a criptografia ponta a ponta (end to end) esteja habilitada, seria possível "espelhar" as conversas travas no aplicativo para outro celular/smartphone ou computador, permitindo que se implementasse ordem judicial de interceptação em face de um usuário específico?
>
> (SUPREMO TRIBUNAL FEDERAL, 2016)

A controvérsia no uso da criptografia ainda está longe de estar finalizada. Por um lado, os aplicadores de lei desejam formas de ter acesso a informações de suspeitos de crimes para constituir provas de suas ações. Por outro lado, os técnicos e os ativistas em direitos humanos chamam atenção para o perigo na criação de formas de "burlar" os mecanismos de criptografia de sistemas, criando algo conhecido como backdoors.

No início desse ano, foi divulgada a existência de uma vulnerabilidade descoberta por Tobias Boelter, um pesquisador da área de segurança da informação da Universidade de Berkeley. Através dessa vulnerabilidade, terceiros ou mesmo a empresa WhatsApp poderiam ter acesso às mensagens trocadas entre dois usuários (THE GUARDIAN, 2017). Com isso, o argumento usado pela empresa para não fornecer dados a Justiça brasileira se tornou questionável, uma vez que o algoritmo criptográfico descrita em seu Technical White Paper (WHATSAPP, 2016) pode não estar corretamente implementado, contendo brechas na segurança que podem ser exploradas.

7. COMBATE AO DDOS

O DoS (Denial of Service) ou negação de serviço é um ataque ativo à segurança de redes. Esse tipo de ataque envolve alguma modificação do fluxo de dados ou a criação de um fluxo falso (STALLINGS, 2015).

Segundo CERT.br (2016) a negação de serviço é uma técnica pela qual um atacante utiliza um equipamento conectado à rede para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Quando usada de forma coordenada e distribuída, ou seja, quando um conjunto de equipamentos é utilizado no ataque, recebe o nome de Ataque Distribuído de Negação de Serviço (DDoS - Distributed Denial of Service). De acordo com Stallings (2015), a negação de serviço impede ou inibe o uso ou gerenciamento normal das instalações de comunicação.

Esse tipo de ataque não visa invadir e nem coletar informações, mas sim exaurir recursos e causar indisponibilidade ao alvo, afetando diretamente os usuários desses recursos que ficam impossibilitados de acessar ou realizar as operações desejadas (CERT.BR, 2016).

Existem diversas formas de se fazer um ataque de negação de serviço, sendo algumas delas: (1) uso de equipamentos infectados, mal-configurados ou invadidos, em que um controlador de botnet envia comandos para que ataquem um alvo específico; (2) exploração de características em serviços de Internet que permitem que um atacante forje o endereço IP da vítima fazendo com que ela receba diversas respostas grandes, as quais consomem uma quantidade considerável de banda da rede; (3) ação voluntária de pessoas que, por intermédio do acesso a sites específicos ou pela instalação de ferramentas, disponibilizam seus computadores para participar dos ataques; e (4) por meio da exploração de vulnerabilidades presentes em serviços e aplicações, geralmente causadas por erros de programação e falhas de configuração (CERT.BR, 2016). Há casos em que o próprio uso normal dos sistemas pode levar à sobrecarga e à consequente lentidão ou indisponibilidade do serviço em questão, o que caracteriza casos não intencionais de negação de serviço. Isso costuma ocorrer por falhas de dimensionamento das aplicações e problemas de escalabilidade de recursos.

Segundo BCP (2012), a técnica chamada de spoofing, ou falsificação de pacotes, é utilizada em ataques de negação de serviço. Essa técnica consiste no uso de pacotes IP com endereços de origem incorretos, que podem ser endereços reservados, ou endereços de redes de terceiros, evitando assim o rastreamento do verdadeiro autor do ataque.

A solução para evitar esse tipo de técnica demanda ações em conjunto entre operadores de redes conectadas à Internet. Os equipamentos responsáveis pela comutação de pacotes IPs devem fazer controle do endereço de origem.

A recomendação descrita em IETF (2000) é para que os pacotes na interface de entrada da rede do provedor sejam filtrados de forma a permitir somente aqueles cujo endereço de origem seja parte da rede conectada àquela interface. Essa solução é conhecida como filtro antispoofing.

Apesar dessa técnica ajudar no combate ao DDoS, ainda é muito difícil fazê-lo, pois há uma dificuldade técnica em se distinguir acessos legítimos de um ataque desse tipo.

De acordo com Stallings (2015), é muito difícil impedir de forma absoluta os ataques ativos, em virtude da grande variedade de potenciais vulnerabilidades físicas, de software e de rede. Em vez disso, o objetivo é detectar ataques ativos e recuperar-se de qualquer rompimento ou atrasos causados por ele. Nesse sentido, CERT.br (2016) diz que toda organização deve planejar com antecedência as ações, tanto técnicas como não

técnicas, a serem tomadas quando o ataque de negação de serviço ocorrer. Esse planejamento inclui as fases de preparação, detecção e análise, mitigação e pós-ataque.

8. CONSIDERAÇÕES FINAIS

O Marco Civil da Internet é uma lei que estabeleceu vários princípios para o uso da Internet no Brasil, dentre eles a privacidade dos usuários. Apesar de não citar nominalmente a questão da segurança da informação pode-se estabelecer paralelos entre a lei e essa área, conforme foi abordado neste artigo.

A apresentação de alguns casos relacionados ao uso de técnicas e tecnologias para garantir a segurança da informação na Internet teve como objetivo elucidar algumas possibilidades a serem consideradas pelas empresas prestadoras de serviço de conexão à Internet. Além disso, algumas controvérsias entre essas práticas e a aplicação da lei foram descritas no artigo.

Ainda se faz necessário que as empresas provedoras de conexão à Internet observem as BCPs, que são publicadas pela IETF, que documentam as melhores práticas relacionadas a uma tecnologia ou ferramenta específica. Muitas delas se relacionam com a área de segurança. Além disso, existem normas técnicas da área de segurança da informação, como a família ISO 27000, que podem ajudar na implementação de medidas para assegurar a privacidade e proteção dos dados pessoais dos usuários.

Contudo, nota-se que o real desafio que deve ser enfrentado para a tutela da privacidade e dos dados pessoais no ambiente da Internet é aliar o direito à tecnologia. Se por um lado a Internet foi genialmente projetada para permitir o compartilhamento livre de informações sem um controle central, essa característica, por sua própria natureza, dificulta em muito a proteção da privacidade e dos dados pessoais.

Há quem argumente que se utilizar da tecnologia como meio de tutela da privacidade tem suas limitações visto que pode ser superada por mecanismos tecnológicos mais avançados ou mesmo mais adequados ao caso. Contudo, tal posicionamento não supera o fato de que o que se busca não é a tutela completa, plena e perfeita. Busca-se a tutela possível por meio de medidas tecnológicas de controle possíveis, capazes de mitigar os riscos, pois sabe-se que eles sempre estarão presentes uma vez que é impossível superá-los.

O que se deve buscar é identificar mecanismos técnicos de proteção disponíveis em segurança da informação que sejam eficientes e que, ao mesmo tempo, estejam de acordo e sejam suportados pelo ordenamento jurídico estabelecido.

Dessa forma, é imprescindível a atuação harmônica e coordenada do direito e da tecnologia. Ao direito cabe tipificar condutas ilícitas, reprimi-las, punindo-as. À segurança da informação cabe identificar as condutas ilícitas tipificadas pelo direito e prevenir ou, na medida do possível, impedir a sua prática por meio de mecanismos técnicos de controle inseridos na arquitetura dos sistemas.

Referências bibliográficas

ALVES, F. M. **Representação criminal e bloqueio de aplicativo**. 2016. Disponível em: <http://omci.org.br/jurisprudencia/115/representacao-criminal-e-bloqueio-de-aplicativo/>. Acesso em: 30 out. 2016.

ANTISPAM.BR. **Como Ocorre o Abuso das Redes**. Disponível em: <http://www.antispam.br/admin/porta25/motivacao/>. Acesso em 17 dez. 2016.

ANTISPAM.BR. **O que é Gerência de Porta 25**. Disponível em: <http://www.antispam.br/admin/porta25/definicao/>. Acesso em 17 dez. 2016.

BCP. Portal de boas práticas para a Internet no Brasil. **Entenda a necessidade do Antispoofing**. 03/12/2012. Disponível em: <http://bcp.nic.br/entenda-o-antispoofing/>. Acesso em 17 dez. 2016.

BRASIL. **Decreto Nº 8.771, de 11 de maio de 2016**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm >. Acesso em: 30 out. 2016.

BRASIL. **Lei Nº 12.965, de 23 de abril de 2014**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >. Acesso em: 30 out. 2016.

CERT.br. **Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS)**. 19/04/2016 Disponível em: <http://www.cert.br/docs/whitepapers/ddos/>. Acesso em 17 dez. 2016.

FONTES, E. **Políticas e Normas para a Segurança da Informação**. Rio de Janeiro: Brasport, 2012.

HOEPERS, C.; FAULHABER, H.; STEDING-JESSEN, K. (Orgs.). **Combate ao spam na Internet no Brasil: Histórico e reflexões sobre o combate ao spam e a gerência da porta 25 coordenados pelo Comitê Gestor da Internet no Brasil**. São Paulo, 2015. Disponível em: <http://www.cgi.br/publicacao/combate-ao-spam-na-internet-no-brasil-historico-e-reflexoes-sobre-o-combate-ao-spam-e-a-gerencia-da-porta-25-coordenados-pelo-comite-gestor-da-internet-no-brasil/>.

IETF. **Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing**. Maio de 2000. Disponível em: <https://tools.ietf.org/html/bcp38>. Acesso em 17 dez. 2016.

INSTITUTO OPERREDE. **Segurança da Informação: um contexto**. Disponível em: < http://www.operrede.com.br/post/87902260210/seguran%C3%A7a-da-informa%C3%A7%C3%A3o-um-contexo >. Acessado em: 30 jan. 2017.

LEONARDI, M. **Tutela e Privacidade na Internet**. São Paulo: Saraiva, 2012. ISBN: 978-85-02-14514-6

LEMOS, R. **O Marco Civil Como Símbolo do Desejo por Inovação no Brasil**. In: LEITE, G. S.; LEMOS, R. (Coords.). Marco Civil da Internet. São Paulo: Atlas. 2014. p.3-11. ISBN 978-85-224-9340-1.

LIMA, C. C. C. **Garantia da privacidade e dados pessoais à luz do Marco Civil da internet**. In: LEITE, G. S.; LEMOS, R. (Coords.). Marco Civil da Internet. São Paulo: Atlas. 2014. p. 148-164. ISBN 978-85-224-9340-1.

MCCUMBER, J. **Information Systems Security: A Comprehensive Model**. Proceedings 14th National Computer Security Conference. National Institute of Standards and Technology. Baltimore, MD. October 1991.

OBSERVATÓRIO DO MARCO CIVIL DA INTERNET - **Íntegra do Acórdão Envio de spam e ausência de interesse de agir**. Disponível em: <http://omci.org.br/jurisprudencia/72/envio-de-spam-e-ausencia-de-interesse-de-agir/> Acesso em: 27 jan. 2017

OBSERVATÓRIO DO MARCO CIVIL DA INTERNET - **Representação criminal e bloqueio de aplicativo**. Disponível em: <http://omci.org.br/jurisprudencia/115/representacao-criminal-e-bloqueio-de-aplicativo/> Acesso em: 27 jan. 2017.

PAESANI, L. M. Garantia Fundamental do não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de Internet, salvo mediante consentimento

livre, expresso e informado ou nas hipótese previstas em lei. In: LEITE, G. S.; LEMOS, R. (Coords.). Marco Civil da Internet. São Paulo: Atlas. 2014. p. 518-526. ISBN 978-85-224-9340-1.

SOLAGNA, F. **A formulação da agenda e o ativismo em torno do Marco Civil da Internet**. 2015.

STALLINGS, W.; BROWN, L. **Computer Security Principles And Practice** – 2ª edição. Prentice-Hall. 2011. ISBN 0-13-277506-9.

STALLINGS, W. **Criptografia e Segurança de Redes: Princípios e Práticas** – 6ª edição. São Paulo: Pearson. 2015. ISBN 978-8543005898.

SUPREMO TRIBUNAL FEDERAL. **Ministro Fachin convoca audiência pública para debater bloqueios judiciais do WhatsApp**. Disponível em: <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=328600>. Acesso em: 17 dez. 2016.

TANENBAUM, A. S.; WETHERALL, D. **Redes de Computadores** - 5ª Edição. São Paulo: Pearson. 2011. ISBN 857605924X.

THE GUARDIAN. **WhatsApp vulnerability allows snooping on encrypted messages**. 13 jan. 2017. Disponível em: < https://cdn.ampproject.org/c/s/amp.theguardian.com/technology/2017/jan/13/whatsapp-backdoor-allows-snooping-on-encrypted-messages >. Acesso em: 29 jan. 2017.

WHATSAPP. **WhatsApp Encryption Overview – Technical White Paper**. 17 nov. 2016. Disponível em: < https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf >. Acesso em: 27 jan. 2017.