PRIVACIDADE ONLINE

PALOMA DE SOUSA CARDOSO

TAINÁ CRISTINA DO NASCIMENTO

DISCIPLINA METODOLOGIA DE PESQUISA I

INSTITUTO FEDERAL DE CIÊNCIA E TECNOLOGIA DE SÃO

PAULO CÂMPUS PIRACICABA

Piracicaba

2019

RESUMO

Neste trabalho serão mostrados conceitos sobre proteção de dados pessoais, de acordo com leis sobre privacidade. Será discutido a importância de um regulamento mais sofisticado, por haver muitas vendas de dados pessoais através de grandes corporações, assim como a existência de meios alternativos para se manter em sigilo na internet, abordando temas como o anonimato na rede *"Deep Web"*, exibindo o funcionamento da criptografia utilizada. Assim como uma conclusão sobre a existência de privacidade na internet.

ABSTRACT

In this work we will show concepts about protection of personal data, according to privacy laws. It will be discussed the importance of a more sophisticated regulation, because there is a lot of sales of personal data through large corporations, as well as the existence of alternative ways to remain in secrecy on the internet, addressing topics such as anonymity in the "Deep Web" network, displaying the operation of the encryption used. As well as a conclusion about the existence of privacy on the internet.

PALAVRAS-CHAVE: Privacidade online; anonimato na internet; deep web.

INTRODUÇÃO

Na temática atual, ainda não há leis e medidas que amparem os usuários de práticas ilícitas de informações sensíveis. Esse problema mundial, levou o país a criar novas leis para cuidarem desse tema, e a função dessa revisão na primeira parte é demonstrar de forma que se faça pensar se futuramente o que foi criado atualmente resolverá alguma coisa

Temos por objetivo destacar as principais leis sobre dados e internet, mostrando suas diferenças e formas de atuação. De forma clara e objetiva, abordaremos sobre Marco Civil da Internet e Lei Geral de Proteção de Dados.

Os estudos realizados à partir deste tema, busca esclarecer dúvidas e incógnitas até hoje não definidas pelo Governo Federal. É de suma importância desmitificar o conhecimento sobre leis que protegem ou não os usuários de vendas de seus dados sigilosos a fim de se ganhar benefícios através dessa prática.

Analisamos a Deep Web e os seus métodos de criptografia para tentarmos concluir se os usuários poderiam navegar com sigilo na internet por meio dessa rede. Contextualizando-a e analisando um caso famoso em que a Polícia foi muito eficiente.

REVISÃO BIBLIOGRÁFICA

REALIDADE DA INTERNET DIANTE DA LEGISLAÇÃO

Marco Civil x LGPD (Lei Geral de Proteção de Dados)

Para falar de leis sobre privacidade de dados, devemos lembrar do Marco Civil da Internet, que atualmente é a normativa que regula as empresas. Esta lei traz aos usuários e provedores de conteúdo e serviços, seus direitos e deveres sobre a Internet mas, não regula dados e como eles são utilizados. Exemplificando, uma pessoa/provedor não pode publicar, postar e agir do jeito que quer na internet. O Marco Civil vem para “monitorar” a forma de como as coisas são feitas na internet, numa visão ética.

Por outro lado, em 14 de agosto de 2018, foi sancionada a LGPD (http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm), que constitui normas de como dados de usuários brasileiros são compartilhados na internet. Até o momento, o Marco Civil não tem autoridade para controlar o compartilhamento de dados sensíveis de cidadãos brasileiros, por isso, a Lei Geral de Proteção de Dados irá regular tudo o que envolver dados críticos.

A *LGPD* prevê:

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de

opinião; IV - a inviolabilidade da intimidade, da honra e da imagem

(Retirado de Lei 12965/2018, Artigo 2, incisos I, II, III, IV)

Direito garantido aos usuários em relação à coleta de dados:

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação;

(Retirado de Lei 12965/2018, artigo 7, VIII “a” e “b”)

Autoridade Nacional de Proteção de Dados (ANPD)

Neste sentido, Diário de Comércio e Indústria (2019, 24/05/2019, 13:00) afirma que “O projeto original da LGPD, aprovado pelo Congresso em julho de 2018, previa a criação da ANPD, que foi vetada por Temer. Quatro meses após o veto, Temer editou a MP 869/2018, que tratava do tema”.

A ANPD seria a agência reguladora que fiscalizaria, requisitaria informações, comunicaria e puniria infratores diante da Lei, outra de suas funções é estar lado a lado com o usuário caso ela decida ou não manter seus dados públicos. Em contrapartida, o crescimento exponencial de dados gerado no país é imenso, e na medida provisória da ANPD não constava como seriam feitos esses tratamentos massivos. Até o exato momento, está sendo discutido na Câmara dos Deputados, a volta desse Agência Reguladora.

As empresas seguem a lei de fato?

Um exemplo prático é, se o seguro de vida detecta que seu cliente tem muitos bens, ele pode oferecer um serviço mais caro, ou, se o plano médico da pessoa descobrir que ela vai muito ao médico, pode aumentar o valor do seu plano de saúde, o que sugere falta de segurança jurídica nos compartilhamentos de dados. O Marco Civil tem por objetivo cuidar do comportamento diante das redes, mas não engloba questões de suma importância atualmente, com isso, as empresas não seguem as leis por falta das mesmas.

Com a implantação da Lei Geral de Proteção de Dados (Lei 12.965/18 - 14 de agosto de 2018), que entrará em vigor em agosto de 2020, as empresas serão

obrigadas a disponibilizar como tratam, armazenam, motivos de coletas e com quem compartilham dados pessoais dos internautas. O que já configura um início de proteção jurídica, dado que se a empresa de seguros de vida quiser compartilhar os dados do cliente para uma empresa de seguros de joias, estará cometendo uma infração de conflito empresarial.

Estamos sempre sendo analisados?

Estamos sendo observados 24 horas por dia, 7 dias por semana, basta olharmos a “seção de Privacidade do Google”, todas as opções de compartilhamento de dados estão ativadas sejam elas voz, geolocalização, históricos de sites, históricos de aplicativos usados no celular ou computador e etc. Empresas como o Facebook, Sites de compras, sites de jogos, aplicativos de celular também utilizam a mesma forma de “espionagem”.

Imagem: Configurações de Privacidade do Google

Termos que aceitamos

Nunca lemos os termos de privacidade antes de entrar num site, aplicativo e etc, mas, o que eles dizem podem ser considerados perigosos para nossos dados pessoais como por exemplo: se você não lê os termos e aceita que o aplicativo tenha acesso ao armazenamento, o que irá ser coletado são os registros de armazenamento ou cartão SD (WRITE_EXTERNAL_STORAGE) e leitura do cartão SD e outros pontos de armazenamento de dados (READ_EXTERNAL_STORAGE)

O que é perigoso: aplicativo pode ler, alterar, ou remover qualquer arquivo no telefone.

Algo que deverá ser reformulado, são termos de Instituições Financeiras, empresas que precisam de contratos, sites na Internet, pois o usuário deverá dar liberdade ou não de compartilhamento de dados. Bancos por exemplo, já compartilham dados sensíveis à outros bancos e/ou empresas, em troca de benefícios, o que à partir do ano que vem, não deverá mais ser feito.

Conclusão acerca da Privacidade provinda de Leis atuais e futuras

Não pode se concluir que há privacidade de dados sigilosos de cidadãos brasileiros, pelo fato de que atualmente não há leis que protejam os usuários e futuramente, a Agência que irá regular o uso de dados brasileiros pode não ser grande o suficiente para “vigiar” uma quantidade tão grande de dados que surgem a cada dia. A situação atual reforça o grande problema em analisar e observar milhares de empresas compartilhando e vendendo dados pessoais e sigilosos das pessoas. O que torna inconclusiva esta pesquisa, pois o que virá futuramente ainda não mostra forças ao combate de vendas de informações.

SERIA A DEEP WEB A SOLUÇÃO PARA A PRIVACIDADE ONLINE?

Contextualizando a Deep Web

O senso comum mais vários sites na internet usa a exemplificação de “camadas” para definir a deep web, sendo que conforme mais profunda for, mais difícil de acessar e mais coisas ilegais/macabras podem ser encontradas. Porém, não é isso do que realmente se trata, além de muitos furos nessas teorias, como o fato de coisas ilegais acontecerem até mesmo na Web comum, como vários casos de pedófilos que assediam crianças em redes sociais e que mantém conteúdo do gênero de pornografia ilegal armazenado (dentre outros inúmeros casos que são anunciados), além de que o termo “difícil” e “macabro” são variáveis, dificuldade é uma questão de conhecimento e prática, enquanto “macabro” pode variar de indivíduo para indivíduo.

De acordo com Michael K. Bergman, popularizador do termo “Deep Web”, em seu artigo “The Deep Web: Surfacing Hidden Value”, publicado em 2001, diz que a deep web é na verdade uma parte da internet que não pode ser encontrada por mecanismos de busca comum, como o “GOOGLE”, no qual ao digitar algo você acessa uma lista de informações sobre o que foi buscado; já nesta rede o acesso funcionaria por meio de uma requisição e então somente a informação especifica seria a encontrada pelo usuário, esta foi a definição primária.

Deep Web nos dias atuais

Atualmente, a deep web é considerada pelos engenheiros da computação, todas as redes que fornecem **anonimato e descentralização**, através de sites que fazem uma **busca por informações não indexadas** pelas redes, ou seja, por meio de requisições a sites específicos, diferentemente do “GOOGLE”.

Para simplificar o termo “indexação”, irá ser utilizado uma breve analogia. Imagine você ir em uma biblioteca (que seria a internet) e não achar certos livros (que seriam os sites) porque a moça (navegador, como o google) não tem acesso a sala onde está o livro (onde está o site/servidor), pois ela não consegue enxergar

através da porta (pois o livro, no caso a informação/site não está indexado). Então para acessar você precisa de uma requisição (como um convite ou fazer um pedido para entrar).

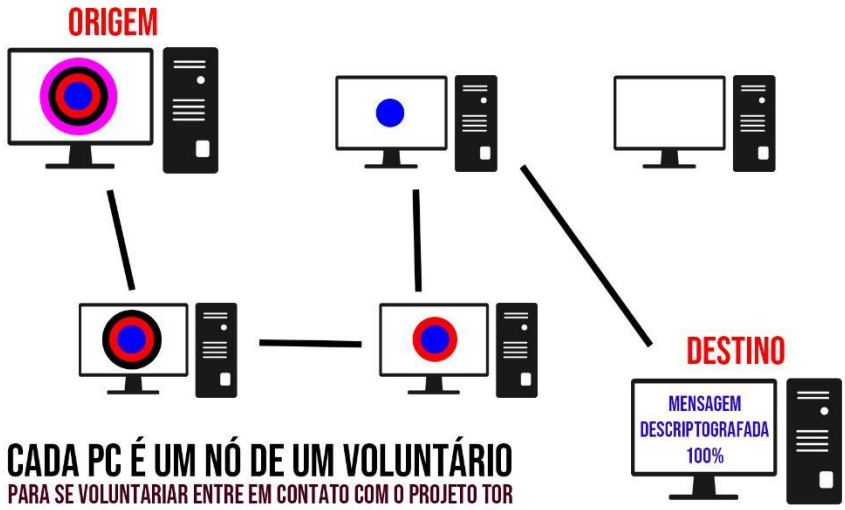
Já o termo “descentralização” é usado para definir informações que circulam a internet, sem possuir um servidor (onde ficam armazenados sites e dados da internet) central. É algo semelhante ao Torrent, alguém faz um upload de um filme na internet e outras pessoas baixam, então esse filme que está no computador de quem baixou, vai ser baixado por outras pessoas, num clico em que para o filme sair da internet precisaria todas as pessoas que já baixaram ele apagá-lo, o que é extremamente difícil de acontecer, pensando em larga escala, porque enquanto um usuário X estiver com o filme, esse filme poderá ser baixado por outras pessoas deste usuário X, isto é a base do conceito P2P (peer-to-peer), que diz que os computadores podem ser usados tanto como cliente, como servidor.

Como funciona o Anonimato?

Utiliza-se softwares para se ter acesso a Deep Web, o mais famoso e utilizado é o TOR (The Onion Router), criado em 2004 em centros de pesquisas militares, com o intuito de ser um sistema que pudesse acessar a internet de forma anônima e descentralizada, garantindo segurança ao usuário. Sendo hoje este software pertencente a uma organização sem fins lucrativos.

O anonimato nele ocorre da seguinte forma: Assim que uma ação é tomada (como o envio de mensagens), ela passará por ‘N’ nós na rede de servidores voluntários que, são pessoas que se voluntariam para o apoio do Projeto TOR, eles tornam os seus computadores em nós, fazendo suas máquinas começarem a agir como cliente-servidor, e então esta ação é camuflada com várias camadas de criptografia, e as camadas vão sendo retiradas uma a uma, até chegar no seu destinatário a mensagem sem nenhuma criptografia, quanto mais servidores voluntários ou nós, mais camadas de criptografia; sendo que esse circuito de redes não pode ser feito no mesmo país, e os caminhos de ida e volta são aleatórios, dentre outras precauções que são demonstradas no site oficial do projeto TOR.

Para simplificar o que foi dito acima, vejamos o exemplo abaixo (cada círculo é uma camada de criptografia):



Posso usar coisas da Web Comum na Deep Web?

Sim, desde que haja uma versão do site para esta rede, você pode. O Facebook tem uma versão “.onion” (uma nomenclatura utilizada nos sites da rede TOR) para ser acessado da Deep Web.

https://facebookcorewwwi.onion/

Uma atitude válida para quem deseja manter sua privacidade na rede, ou até mesmo para quem mora em países com altas restrições poder navegar no site.

Tem como quebrar o anonimato?

A maneira mais comum é o **usuário** tornar sua segurança vulnerável, não tomando as devidas precauções para se manter no anonimato, um exemplo de atitude vulnerável, seria o usuário fazer um download, sem ter noção do que ele está fazendo, isso poderia comprometer sua localização.

Através de iscas da polícia e infiltrados é possível também obter a localização de um indivíduo, se ele cair na armadilha, além de métodos como vírus, invasões ou tentativas de achar vulnerabilidades que a polícia pode utilizar.

Porém a quebra do sigilo dificilmente ocorrerá por falhas do sistema de anonimato utilizado na Deep Web, na maioria dos casos é necessária uma vulnerabilidade que o próprio usuário tenha deixado.

Silk Road

Um caso que ficou famoso em 2013, sendo um dos grandes atos da Polícia neste meio, foi o derrubamento do site Silk Road que vendia drogas no TOR, mais a prisão perpétua de seu criador Ross William Ulbricht, as faturas afirmam que o site chegou a movimentar mais de 1 bilhão de dólares em vendas. O FBI declarou que foi falha na página de login do site, porém muitas pessoas e pesquisadores como Nik Cubrilovic discorda da explicação e afirma que: “muitas pessoas monitoravam a Silk Road e ninguém percebeu essa falha. Para o especialista, a explicação do FBI tenta ocultar o que realmente aconteceu: a exploração pelo FBI de uma falha de segurança existente na Silk Road. A brecha fazia com que o site retornasse diversas informações, entre elas o endereço de IP. O FBI tem uma boa razão para não mencionar qualquer erro ou afirmar que forçou o servidor a fazer algo, fingindo que eles simplesmente pegaram o IP da conexão já que isso levantaria questões sobre a legalidade das ações que levaram à descoberta do IP” (Retirado do Portal G1 da Globo - 11/09/2014).

CONCLUSÃO

A deep web seria a solução para obter privacidade na internet? Sim, no caso de manter sigilo de seus dados pessoais e evitar que eles sejam vendidos na internet comum, a deep web é sim uma solução. Já em casos que o indivíduo queira cometer atos ilegais na rede, não é possível concluir que ele conseguirá a mesma privacidade de um usuário que não é criminoso.

REFERÊNCIA BIBLIOGRÁFICA

Cordeiro, B. S. e Gouveia, B. L. , Regulamento Geral de Proteção de Dados. (RGPD): o novo pesadelo das empresas? Maio, 2018, UFP.

https://observador.pt/especiais/silk-road-como-caiu-o-imperio-de-droga-na-internet-que-valia-12-mil-milhoes/

https://jornalggn.com.br/sites/default/files/documentos/2011_bergman_7_cafarella_informationretrieval_presentation1_2.pdf

http://brightplanet.com/wp-content/uploads/2012/03/12550176481-deepwebwhitepaper1.pdf

https://commons.wikimedia.org/wiki/File:Silk_Road_Seized.jpg

https://www.vice.com/pt_br/article/8q5yxp/como-o-fbi-encontrou-os-servidores-do-silk-road

http://g1.globo.com/tecnologia/noticia/2014/09/explicacao-dada-pelo-fbi-para-encontrar-silk-road-gera-polemica.html

https://tecnoblog.net/141789/silk-road-ross-ulbricht-preso/

https://www.gta.ufrj.br/grad/11_1/tor/index.php?file=kop2.php

http://www.fabricadenoobs.com.br/deep-web/redes-documentadas/onion/

http://g1.globo.com/tecnologia/blog/seguranca-digital/post/saiba-como-o-site-de-venda-de-drogas-silk-road-se-escondia-na-web.html

https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2019/03/14/deep-web-entenda-o-que-e-e-os-riscos.ghtml

http://labs.siteblindado.com/2019/03/desmistificando-deep-web-um-guia-basico.html?m=1

https://www.vivaolinux.com.br/topico/vivaolinux/Tor-estou-anonimo