Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

VINICIUS LONGO MACHADO

INFORMAÇÃO QUE COMPARTILHAMOS: UMA ANÁLISE SOBRE A PRIVACIDADE ONLINE

Assis/SP

2020

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

VINICIUS LONGO MACHADO

INFORMAÇÃO QUE COMPARTILHAMOS: UMA ANÁLISE SOBRE A PRIVACIDADE ONLINE

Projeto de pesquisa apresentado ao Curso de Ciência da Computação do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientando(a): Vinicius Longo Machado
Orientador(a): Prof. Me. Fabio Eder Cardoso

Assis/SP

2020

FICHA CATALOGRÁFICA

M149i MACHADO, Vinicius Longo
Informação que compartilhamos: uma análise sobre a privacidade online / Vinicius Longo Machado. – Assis, 2020.

48p.

Trabalho de conclusão do curso (Ciência da Computação). – Fundação Educacional do Município de Assis-FEMA

Orientador: Me. Fábio Éder Cardoso

1.Privacidade 2. Anonimato

CDD005.8

INFORMAÇÃO QUE COMPARTILHAMOS: UMA ANÁLISE SOBRE A PRIVACIDADE ONLINE

VINICIUS LONGO MACHADO

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

Orientador:

Prof. Me. Fabio Eder Cardoso

Examinador:

Prof. Dr. Alex Sandro Romeo de Souza Poletto

RESUMO

Privacidade e anonimato na Internet, vem se tornando temas cada vez mais discutidos nos dias de hoje. Com cada vez mais pessoas utilizando a Internet no dia a dia, a manipulação de dados pessoais, roubo de informação, rastreamento de tráfego e diversas outras atividades, estão se tornando cada vez mais comuns. Esta pesquisa tem como objetivo divulgar tecnologias que podem ser utilizadas para reverter tais atividades e trazer de volta para o usuário a autonomia de controlar suas próprias informações.

Palavras-chave: Privacidade, anonimato, internet, informação.

ABSTRACT

Privacy and anonymity on the internet, became even more discussed topics nowadays. With even more people browsing the web on a daily basis, things like personal data manipulation, information theft, data tracking amongst other activities have become even more common. This research has the objective to spread awareness about all of those activities and also show different types of tools and technologies to fight against them and bring back to the user the autonomy to control their own information.

Keywords: Privacy, anonymity, internet, information.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1. INTRODUÇÃO

Dizer que você não se importa sobre o direito à privacidade porque você não tem nada a esconder, é como dizer que você não se importa com a liberdade de expressão porque não tem nada a dizer. (SNOWDEN 2015)

Atualmente com a grande abrangência da Internet na vida das pessoas, um tópico muito discutido é o da privacidade. Seguindo esse preceito, será realizada uma análise do tipo de informação, que, com ou sem consentimento, pode ser disponibilizada online, e que podem ser acessadas, analisadas e manipuladas por terceiros.

Apenas no primeiro semestre de 2018, foram contabilizadas, ao todo, cerca de 4,55 bilhões de registros de dados comprometidos no mundo todo, um número 133% maior do que no mesmo período no ano anterior, dentre desses, cerca de 56% das violações de dados foram provenientes de mídias sociais. (BUTCHER 2018). Considerando essa informação, fica evidente que, os dados dos usuários não estão seguros como o esperado.

Com o aumento da preocupação a respeito desse assunto, nos últimos anos, foram desenvolvidas diversas ferramentas, serviços e *softwares* com o intuito de garantir ao público uma maior privacidade ao acessar a Internet. Como por exemplo o TOR (*The Onion Routing*), que é uma rede aberta e livre baseada no protocolo SOCKS[1] e projetada para alcançar o anonimato de aplicações que utilizam o "*Transport Layer Protocol*" (TCP), através da sobreposição de camadas de criptografia. (DINGLEDINE et al. 2014)

Levando isso em conta, este trabalho propõe uma pesquisa com o objetivo de avaliar a conhecimento do público em geral a respeito do assunto, além de apresentar métodos eficientes para que se possa garantir um acesso privado à Internet.

[1] SOCKS é um protocolo de internet que troca pacotes de rede entre cliente e servidor através de um proxy.

Para finalizar será feita uma análise a respeito da lei geral de proteção de dados pessoais, prevista para entrar em vigor em agosto de 2020 e como esse fato afetará tanto usuários comuns e indivíduos que armazenam informação.

1.1 OBJETIVOS

Os objetivos deste trabalho são, através da pesquisa, esclarecer para o público em geral questões a respeito da privacidade e anonimato *online*. Demonstrar como a informação é obtida. Por meio de uma pesquisa, entender qual é o conhecimento do público geral a respeito da privacidade e de como seus dados são manipulados. Descrever métodos para que se tenha uma garantia maior de privacidade, além de como navegar anonimamente.

1.2 JUSTIFICATIVAS

A importância deste estudo está na necessidade de o público entender, que em muitas ocasiões, suas informações pessoais podem ser usadas para classificar seu perfil. Com tais informações é possível determinar, por exemplo, perfil de consumo e então determinar preços de produtos de acordo com o indivíduo. Outra possibilidade seria determinar a localização do usuário para que publicidade agressiva seja divulgada para um público seleto.

Portanto, sabendo dessas informações, um usuário comum pode mitigar essas ações, e ter uma “vida virtual” consideravelmente mais segura e privada.

1.3 MOTIVAÇÃO

A principal motivação para este trabalho surgiu com a preocupação em como os nossos dados são usados “contra”, nós, usuários, em diversos tipos diferentes de serviços que utilizamos todos os dias, como por exemplo, redes sociais, lojas virtuais e mecanismos de busca.

Outro motivo, também muito relevante e a respeito da segurança aplicada em servidores em que nossos dados são armazenados que podem estar vulneráveis a possíveis ataques com o intuito de os roubar.

Com esse tipo de informação é possível gerar uma conscientização com o público para que cada vez menos pessoas tenham seus dados roubados ou comprometidos.

1.4 PERSPECTIVAS DE CONTRIBUIÇÃO

Este trabalho pode vir a ajudar, tanto o público em geral, assim como profissionais da área de tecnologia a ter suas dúvidas esclarecidas a respeito da informação que compartilhamos, além de conscientizar sobre o uso responsável de serviços online. Outra possibilidade seria de possivelmente mostrar para grandes corporações que armazenam grande quantidade de dados sensíveis, como o público se preocupa com sua privacidade.

Além disso, este estudo pode vir a servir como uma introdução mais direta ao assunto, para que futuros interessados em se aprofundar ainda mais possam ter uma base para começar seus próprios estudos.

1.5 METODOLOGIA DE PESQUISA

Para o desenvolvimento deste trabalho, serão utilizadas diversas fontes para uma pesquisa descritiva com o uso da técnica de estudo de caso. Será também desenvolvida um questionário utilizando a ferramenta Google forms, para entender a preocupação do público a respeito da privacidade, neste questionário, serão apresentadas uma serie de situações a respeito da privacidade na internet onde o participante deve indicar seu nível de preocupação com uma nota de 1 a 7, com essas notas será feita uma análise do perfil do usuário. Além disso, ao final será apresentado o cenário ideal de privacidade, ou seja, mostrando como e com quais tipos de ferramentas e tecnologias é possível obter esse resultado.

1.6 ESTRUTURA DO TRABALHO

A estrutura deste trabalho é composta das seguintes partes:

- **Capítulo 1 – Introdução:** Neste capítulo é contextualizada a área de estudo e apresentará os objetivos, justificativas, motivação, perspectivas de contribuição e metodologia de pesquisa para o desenvolvimento deste trabalho.
- **Capítulo 2 – Privacidade e anonimato:** Neste capítulo, é feita uma breve introdução sobre o conceito de privacidade e o anonimato além da importância dos mesmos para garantir segurança e autonomia na internet.
- **Capítulo 3 – VPN:** Neste capítulo, é contextualizada a tecnologia de VPN, seu funcionamento, proposta de uso e como pode nos ajudar a manter o anonimato.
- **Capítulo 4 – Rede TOR:** Neste capítulo, é apresentada a tecnologia da rede TOR e como ela vem sendo usada para garantir maior segurança para comunicação além de acessos mais privados.
- **Capítulo 5 – LGPD**: Neste capítulo, será abordada a LGPD (Lei Geral de Proteção de Dados Pessoais) e como ela afetará o armazenamento de nossos dados e também como poderão ser utilizados.
- **Capitulo 6** – **Pesquisa:** Neste capitulo, é elaborada uma pesquisa com o público, a fim de entender o perfil do usuário a respeito de sua privacidade.

- **Capitulo 7** – **Cenário Ideal:** Neste capitulo será discutido, um possível cenário ideal de privacidade e/ou anonimato na internet, abordando ações que podem ser tomadas tanto pelo usuário como por organizações ou entidades na internet.
- **Capítulo 8 – Considerações finais:** Neste capítulo, conclui-se o desenvolvimento do trabalho com um breve resumo do que foi realizado, além de possíveis vantagens de uma navegação mais privativa.
- **Referências**

2. PRIVACIDADE E ANONIMATO

Privacidade e anonimato são dois elementos principais para proteger a liberdade de expressão. O objetivo do anonimato é o de proteger toda a informação que pode revelar a identidade real do usuário, informação como nome, localização, endereço de IP e etc. O objetivo da privacidade é o de garantir que qualquer organização ou entidade não coletem ou armazenem quaisquer informações privadas como histórico de navegação, informações de localização, detalhes de contas, entre outras, sem o conhecimento ou autorização do usuário.

2.1 CONCEITOS

O conceito de privacidade e *online* refere-se à privacidade pessoal a que se tem direito quando exibe, armazena ou fornece informações sobre você mesmo na Internet, o que pode incluir informações de identificação pessoal assim como informações não pessoais, como seu comportamento em um determinado site. Sem essa privacidade, suas atividades estão sujeitas a serem coletadas e analisadas por terceiros. (LEITE 2016)

A privacidade na internet toma diversas formas, incluindo declarações de privacidade em *websites*, controle de compartilhamento de dados, iniciativas de transparência de dados e outras.

Privacidade e anonimato são fundamentais para os usuários, especialmente com o grande crescimento do *e-commerce. Violações de privacidade e o risco de ameaças são considerações padrões para qualquer site em desenvolvimento.*

2.2 IMPORTÂNCIA DA PRIVACIDADE

A privacidade é um dos conceitos mais importantes de nosso tempo, mas ainda assim é um conceito praticamente “enganoso”, levando em conta a rápida evolução da tecnologia, que faz com que cada vez mais informação e em maior quantidade seja coletada, armazenada e utilizada de forma a atingir objetivos que podem ser tanto benéficos ou maléficos.

Em um possível caso de vazamento de informação, muitos desses dados podem prejudicar os indivíduos envolvidos de diversas formas, como por exemplo dados sensíveis, como números de documentos, dados financeiros, dados de saúde, endereços ou até informação como religião, orientação sexual e etnia.

Com uma maior garantia de privacidade na internet, cada individuo tem, consequentemente, sua liberdade e segurança garantidas, considerando que o possível uso indevido de suas informações pode vir a gerar possíveis pré-conceitos.

3.VPN

Uma rede virtual privada cria uma conexão segura e encriptada sobre uma rede menos segura, normalmente a internet, permitindo que usuários acessem diferentes aplicações e recursos em redes remotas. Para garantir a segurança, os dados viajam através tuneis seguros utilizando métodos de autenticação, incluindo senhas, tokens e outros métodos de identificação únicos. A segurança de dados de VPNs permanece constante através de dados encriptado e protocolos de tunelamento. A principal vantagem de uma VPN é que ela oferece uma alternativa mais barata que uma alternativa como uma WAN (Wide Area Network) privada.

VPNs são primariamente utilizadas para:

- Proteção contra crimes virtuais em redes desconhecidas ou com menos segurança.
- Conseguir privacidade, escondendo atividades online de provedores de internet.
- Contornar medidas de censura.
- Acobertar o uso de serviços P2P (Peer to peer), como torrents e outros.

3.1 INTRODUÇÃO

VPN ou *Virtual Private Network* (Rede Privada Virtual) consiste de uma rede privada construída sobre uma rede pública que permite aos usuários enviar e receber dados através de redes públicas ou compartilhadas como se seus dispositivos estivessem conectados diretamente a uma rede privada. Dessa forma, aplicativos sendo executados em dispositivos conectados em uma VPN podem se beneficiar da funcionalidade e segurança da rede privada.

Apesar desse uso mais “corporativo”, o tipo de VPN que será abordado é para o acesso à Internet onde ela só precisa, através de um protocolo de tunelamento, transportar o tráfego do cliente para outra localidade de forma segura e encriptada, dessa forma não há como dispositivos de usuários conectados na mesma “VPN” possam ser visualizados. Essas VPNs podem ser baseadas em simples protocolos de VPN ou outros métodos considerados mais “camuflados” assim como protocolos proxy.

3.2 FUNCIONAMENTO

VPNs utilizam o protocolo de tunelamento (um protocolo de comunicação) para transferir dados através da internet como se fosse uma rede privada. Para tal, o tunelamento encapsula pacotes de IP junto a um novo cabeçalho de IP, o cabeçalho original que foi empacotado contém o IP de destino (privado) enquanto a nova camada do pacote contem como destino o endereço publico do servidor de VPN.

De forma bem simplificada, uma VPN conecta seu dispositivo a um servidor e permite que o usuário possa acessar a Internet por meio da conexão do servidor, dessa forma, se o servidor estiver localizado em outro país, para o serviço que o usuário está conectado parecerá que o usuário está neste determinado país.

Dessa forma é possível obter uma conexão mais privativa já que seus dados de navegação serão criptografados durante o trajeto. (Chin 1998)

3.2.1 PROTOCOLOS DE TUNELAMENTO COMUNS

- PPTP
- IPSec IKEv2 (*Internet key Exchange version 2*).
- *OpenVPN.*

PPTP (*Point-to-point tunelling protocol* ou protocolo de tunelamento ponto a ponto) é um protocolo básico, porem obsoleto baseado em PPP (*Point-to-point protocol*). A especificação do protocolo PPTP não descreve funções de criptografia ou autenticação e depende do protocolo PPP ser tunelado para implementar sua função de segurança. A carga do PPP é encriptada utilizando o protocolo de ponto a ponto da Microsoft (MPPE), que implementa um algoritmo de criptografia que produz chaves com um máximo de 128 bits por seção.

IKEv2 é parte do protocolo IPSec, padronizado em RFC 7296. IPSec se tornou o protocolo padrão para comunicação segura pela internet, provendo confidencialidade, autenticação e integridade. O protocolo IKEv2 implementa um grande numero de algoritmos de criptografia, incluindo 3DES, AES, Blowfish, Camellia entre outros.

OpenVPN é um protocolo de VPN de código aberto desenvolvido pela empresa de mesmo nome. É muito popular, porem não é baseado em padrões como RFC. Utiliza um protocolo de segurança customizado e SSL/TLS para troca de chaves além de prover completa confidencialidade, autenticação e integridade. A OpenVPN utiliza a biblioteca OpenSSL para oferecer criptografia, a OpenSSL implementa um grande numero de algoritmos de criptografia como 3DES, AES, RC5, Blowfish.

4. REDE TOR

O projeto TOR foi iniciado em 1995 pelo Laboratório de pesquisa naval dos EUA. Seu principal objetivo era o de separar informação de identificação do roteamento e de desenhar uma rede de comunicação anônima para uso militar. Após ser revelada ao público, foi amplamente estudada, levando a diferentes revisões do projeto. De acordo com a ultima divulgação do Tor metrics, atualmente existem mais de 2.5 milhões de usuários ativos do Tor com quase 6500 nós de retransmissão transportando trafego e provendo quase 30 Gbps de largura de banda para a rede Tor.

4.1 INTRODUÇÃO

O Tor pode ser classificado como um sistema de aumento de privacidade, que foi feito para proteger a privacidade de usuários da internet de possíveis analises de trafego.

Tor é um software grátis e de código aberto que permite comunicação anônima. O nome deriva do projeto do software original "*The Onion Router*", por "onion" (cebola em inglês) entende-se a característica de camadas, como as diferentes camadas de uma cebola, mas neste caso as diferentes camadas são utilizadas para encobrir diferentes vias de trafego. O Tor direciona tráfego da Internet por uma rede mundial de voluntários composta de mais de sete mil pontos para esconder a localização do usuário e protegê-lo de qualquer indivíduo que possa estar conduzindo uma análise de tráfego ou monitoramento de rede. Usar o Tor torna mais difícil de rastrear atividades online ao usuário, o que inclui acessos a *websites*, mensagens e outras formas de comunicação. O uso previsto do Tor é para proteger a privacidade dos usuários, assim como sua liberdade e direito de ter uma comunicação confidencial, mantendo suas atividades *online* e sem monitoramento.

4.2 FUNCIONAMENTO

A rede TOR percorre servidores de milhares de voluntários ao redor do mundo. Os dados são criptografados em um pacote quando entra na rede TOR, então diferente de conexões tradicionais a rede TOR remove parte do cabeçalho do pacote, onde parte da informação que pode ser utilizada para identificar o remetente pode ser encontrada. (Tor Project, 2019)

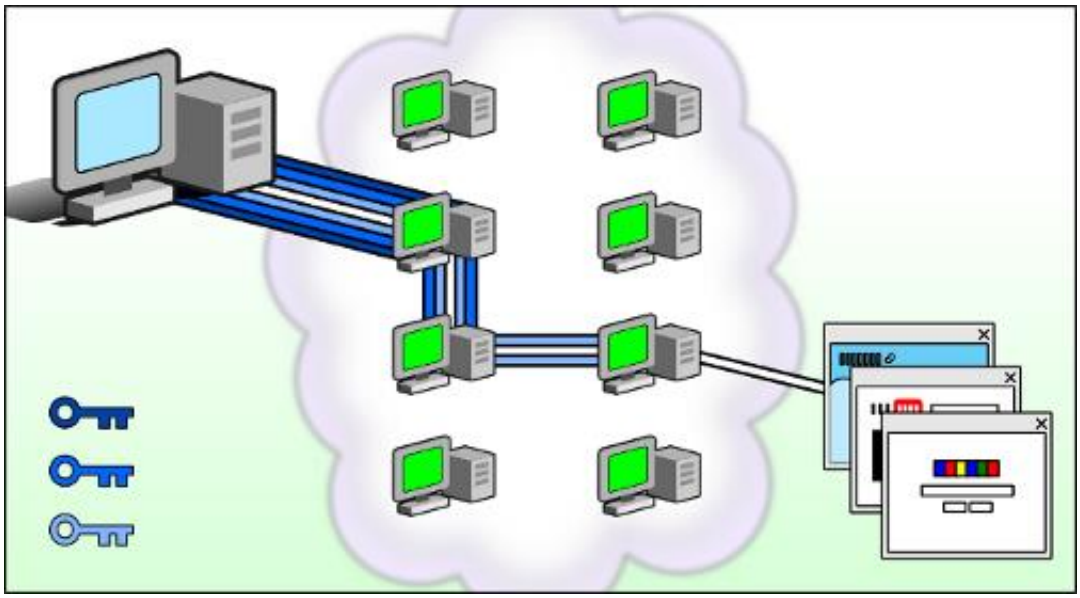

Figura 1 - Funcionamento da rede TOR (Tor Project, 2020)

O pacote modificado e criptografado é então enviado através de muitos desses servidores em direção a seu destino final.

Cada servidor descriptografa somente o mínimo necessário do pacote de dados para saber de qual servidor a informação chegou e para qual ele deve enviar, o servidor então reempacota os dados e os envia.

Para que todo esse processo seja simplificado para o usuário final o TOR Project (organização que mantém o funcionamento do serviço) desenvolveu o Tor browser,

que através de uma versão modificada do navegador Mozilla Firefox, com algumas funções extras para o anonimato e privacidade. Algumas dessas funções são o *Tor Launcher*, *Tor button*, *no script* e *HTTPS-Everywhere.* Por padrão, a navegação é configurada para o modo privado com a opção de limpar a atividade de navegação e seus "artefatos" relacionados como cookies e outros dados relacionados a navegação, assim que o navegador é encerrado.

4.3 CONCLUSÃO REDE TOR

Em uma visão geral sobre a rede TOR, nota-se que por meio de seu uso, é possível ter uma garantia maior de que nossos dados estão navegando por uma rota mais segura, impedindo que terceiros tenham acesso a informações como localização, sistema operacional, serviço provedor de Internet, além de dificultar o mapeamento e classificação de nosso padrão de uso da *web*.

5. LGPD

A LGPD, Lei Geral de Proteção de Dados (Lei Federal 13.709/18) tem como objetivo garantir o direito à privacidade e a proteção de dados pessoais, estabelecendo regras claras e transparentes a respeito do armazenamento e da manipulação de dados pessoais.

A lei também garantirá uma ampliação de direitos para o titular dos dados.

5.1 SOBRE A LEI

A LGPD, que entrará em vigor no dia 20/08/2020 define como dado pessoal, qualquer informação relacionada a pessoa natural identificada ou identificável, ou seja, qualquer dado que possa ser usado para identificar um indivíduo. A lei tem como objetivo garantir e proteger os direitos de liberdade e privacidade assim como o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018), que tenham suas informações armazenadas por organizações, sendo o individuo usuário dela ou não.

No art. 2º da LGPD são listados sete fundamentos da característica de proteção de dados, como respeito a privacidade. No art. 6º são listados princípios que guiam o tratamento de dados, precedidos, principalmente, pela boa fé, como é determinado no caput. A tabela 1 mostra os princípios abordados.

#	Princípio e sua definição
I	**Finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II	**Adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III	**Necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IV	**Livre acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V	**Qualidade dos dados:** garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI	**Transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII	**Segurança:** utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII	**Prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX	**Não discriminação:** impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X	**Responsabilização e prestação de contas:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Tabela 1 - Princípios da LGPD (BRASIL, 2018)

Uma de suas maiores características é regularizar o tratamento de dados pessoais estabelecendo justificativas que dão direito a uma empresa tratar dados. Essas justificativas são parte importante de como funciona a LGPD pois, através delas é possível delimitar uma linha entre o tratamento legal e ilegal de dados. As justificativas para o tratamento de dados devem ser destacadas como o consentimento, determinando que, se uma empresa deseja usar o consentimento do usuário como justificativa, ela deve fazer de forma clara e objetiva, ao contrário do método atual que utiliza de entrelinhas de termos e condições. (BRASIL, 2018)

5.2 COMO SERÁ APLICADA

No capitulo VIII da lei é abordado o assunto da fiscalização e consequentemente sanções administrativas que podem ser aplicadas pela violação da lei. Essas sanções variam entre advertência, com indicação de prazo para adoção de medidas corretivas, multa de até 2% do faturamento da pessoa jurídica limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração cometida, além de multas diárias e outras punições (BRASIL, 2018).

Para garantir o cumprimento da lei, no art. 55-A fica registrado a criação da Autoridade Nacional de Proteção de Dados (ANPD), um órgão da administração publica federal, integrante da Presidência da República. A ANPD é assegurada autonomia técnica e decisória, para a tomada de decisões. Na tabela 2 ficam registradas as competências da ANPD como descritas pelo art. 55-J

#	**Competências**
I	Zelar pela proteção dos dados pessoais, nos termos da legislação;
II	Zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei;

III Elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;

IV Fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;

V Apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;

VI Promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;

VII Promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;

VIII Estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;

IX Promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;

X Dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial;

XI Solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei;

XII Elaborar relatórios de gestão anuais acerca de suas atividades;

XIII Editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei;

XIV Ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;

XV Arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas;

XVI Realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;

XVII Celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942;

XVIII Editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei;

XIX Garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso);

XX Deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos;

XXI Comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;

XXII Comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal;

XXIII Articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação;

XXIV Implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei.

Tabela 2 - Competência da ANPD (BRASIL, 2018)

De forma resumida, a ANPD deve atuar na fiscalização dos agentes de tratamento de dados, assim como na instrução dos titulares, assim como mencionado no item VI da tabela 2, o que deve, de certa forma levar ao conhecimento da população quais são os seus direitos a respeito de sua privacidade.

A LGPD mostra um grande avanço a respeito do cenário de segurança de dados no Brasil, visto que é a primeira lei no Brasil a lidar com o assunto, proporcionando ao usuário o controle de seus dados pessoais e privacidade, por meio de regras claras que ditam como devem ser tratados seus dados pessoais.

6. PESQUISA

De modo a entender a atitude atual do público a respeito da privacidade online, uma pesquisa aplicada através do *google forms* foi divulgada em diferentes redes sociais e recebeu um total de 889 respostas. A pesquisa incluiu perguntas que avaliavam a preocupação dos usuários da internet com a privacidade em diferentes situações que podem ser vivenciadas online (o foco das situações foi nos casos em que o indivíduo tem mais controle sobre a informação), a pesquisa também avaliou a taxa de uso da internet pelos usuários, além de algumas informações demográficas.

6.1 MEDIDAS DA PESQUISA

A preocupação com a privacidade foi avaliada utilizando 15 diferentes declarações que refletem cenários que representam 5 diferentes premissas da privacidade que foram identificadas pela literatura, além delas, foram apresentados 6 diferentes comportamentos que um usuário pode vir a apresentar em seu dia-a-dia na internet em relação a sua privacidade. A primeira premissa é a percepção sobre a coleta de dados, ela sugere que os usuários ficam menos preocupados a respeito da privacidade quando eles estão cientes que seus dados são coletados do que quando os dados são coletados sem seu conhecimento (Nowak & Phelps, 1995). A segunda premissa, uso de informação, sugere que consumidores são menos preocupados com sua privacidade quando seus dados são utilizados apenas para o propósito de uma única transação, e a preocupação aumenta junto com o uso da informação além da transação original (Nowak & Phelps, 1995). A terceira premissa, sensibilidade da informação, sugere que a coleta de alguns dados (como o nome, por exemplo) causa menos preocupação a respeito da privacidade do que de outros dados como números de documentos (Milne, 1997). A quarta premissa é a familiaridade com a organização, esta, sugere que os usuários se preocupam menos com sua privacidade quando são familiares com a organização que faz a coleta de dados e consequentemente a preocupação aumenta quando não se tem

familiaridade com a organização. A última premissa, compensação, sugere que a preocupação com a privacidade diminui quando os usuários recebem algo de valor em troca da informação que eles entregam as organizações (Milne & Gordon, 1993).

Para cada premissa, três diferentes situações foram apresentadas, uma refletindo um tipo de situação que, em média, causaria um baixo índice de preocupação com a privacidade, uma que em média causaria um nível moderado de preocupação com a privacidade e uma terceira que, em média, causaria um alto nível de preocupação. Essas 15 situações foram adaptadas de estudos anteriores sobre a privacidade num contexto "*offline*" (Nowak & Phelps, 1995) para um "*online*", ou desenvolvidas a partir de pretextos existentes.

Situações (Preocupação com a privacidade em cada situação medida utilizando uma escala de 1 a 7 onde 1 = Nem um pouco preocupado e 7 = Extremamente preocupado).

- Percepção
    - Você recebe um e-mail de um site que você se registrou no passado (Preocupação baixa).
    - Você recebe um e-mail de um site que você visitou no passado (Preocupação moderada).
    - Você recebe um e-mail e não sabe de onde a organização conseguiu o seu endereço (Preocupação alta).

- Uso
    - Um site pede o seu endereço de e-mail apenas para lhe enviar informação de interesse (Preocupação baixa).
    - Um aviso no site diz que a informação coletada pode ser utilizada pela empresa (Preocupação moderada).
    - Um aviso no site diz que a informação coletada pode ser vendida para outras empresas (Preocupação alta).

- Sensibilidade
    - Seu nome é requisitado para acessar determinada área do site

(Preocupação baixa).
    - Informações como preferências e outros dados pessoais são requisitados para acessar o site (Preocupação moderada).
    - Seus números de RG e/ou CPF são requisitados para acessar (Preocupação alta).

- Familiaridade
    - Você recebe um e-mail sobre um novo produto de uma empresa que você já comprou anteriormente (Preocupação baixa).
    - Você recebe um e-mail de um novo produto de uma empresa conhecida, porém que você nunca comprou antes (Preocupação moderada).
    - Você recebe um e-mail sobre um novo produto de uma empresa que você nunca ouviu falar (Preocupação alta).

- Compensação
    - Um site pede o seu endereço de e-mail para acessá-lo, no momento do cadastro, você estará participando do sorteio de um novo celular (Preocupação baixa).
    - Um site pede o seu endereço de e-mail para acessá-lo, no momento do cadastro você receberá um cupom de 10% de desconto para compras futuras (Preocupação moderada).
    - Um site pede o seu endereço de e-mail para acessá-lo, no momento do cadastro, você receberá uma caneta de brinde (Preocupação alta).

Comportamentos (Frequência com que o usuário realiza cada ação utilizando uma escala de 1 a 7 onde 1 = Nunca fiz e 7 = Sempre faço).

- Leitura de e-mails não solicitados.
- Registro em sites.
- Prover informações falsas ao se registrar em um site.
- Prover informações incompletas ao se registrar em um site.
- Pedir a de inscrição de listas de e-mail
- Enviar mensagens negativas para organizações que enviam e-mails não

solicitados.

As 15 afirmações e 6 comportamentos foram apresentados juntos com a instrução de indicar seu nível de preocupação com a privacidade usando uma escala bipolar de sete pontos sendo de 1 (nem um pouco preocupado) a 7 (extremamente preocupado). Em adição as afirmações em relação privacidade, os participantes também foram classificados de acordo com sua taxa de uso da internet e demografia. A seção de demografia concluiu a pesquisa e mediu gênero, idade e escolaridade.

6.2 AMOSTRA

A tabela 1 mostra a demografia e o nível de uso da internet dos 889 participantes. Aproximadamente 70% dos participantes são homens e 42% têm idade entre 18 e 34 anos. Os participantes têm um alto nível escolaridade sendo que 60% possuem ensino superior completo.

Características demográficas		**Percentual de participantes**
Gênero	**Masculino**	70,4%
	Feminino	29,6%
Idade	**18 - 24**	16,7%
	25 - 34	25,5%
	35 - 44	27,3%
	45 - 54	20,4%
	55 - 64	7,1%
	65+	3%
Grau de escolaridade	**Ensino médio completo**	38,7%
	Ensino superior completo	40%
	Mestrado	15,7%
	Doutorado	5,6%
Adota uma identidade alternativa enquanto online	**Sim**	28,6%
	Não	71,4%
Percentual de tempo na internet por local de acesso	**Casa**	72,8%

	Trabalho	22%
	Escola	4,1%
	Outro	1,1%
Frequência que checa e-mails	**Diversas vezes no dia**	66,2%
	Uma vez ao dia	20,7%
	Diversas vezes na semana	11,2%
	Uma vez por semana	1,7%
	Menos de uma vez por semana	0,2%

Tabela 3 - Perfil dos participantes (n = 889)

6.3 RESULTADOS

Como um primeiro passo, foi efetuada uma classificação dos participantes baseada na tipologia de Westin, para tal, uma variável chamada de “preocupação total” foi criada. Essa variável resume cada uma das notas geradas pelos participantes. Essa nota de preocupação varia entre 15 e 105, uma nota de 15 representa um indivíduo para qual nenhuma das 15 situações representou qualquer tipo de preocupação, enquanto uma nota de 105 representa um indivíduo que para todas as situações se sentiu extremamente preocupado. A média total da nota foi de 58.86, com um desvio padrão de 18.93.

A nota da preocupação total foi utilizada para segmentar os participantes em três diferentes grupos que espelham a tipologia de Westin. Participantes que apresentaram uma nota entre 15 e 30 foram classificados como o grupo “despreocupado” de Westin, para esses participantes as 15 situações aparentaram causar um nível mínimo de preocupação. Cerca de 16% dos participantes fazem parte desse grupo de consumidores virtuais, comparados com 25% no estudo de Westin.

Participantes que possuem uma nota entre 31 e 89 foram classificados como “pragmáticos” seguindo a tipologia de Westin, esses participantes possuem níveis de preocupação com a privacidade que variam de acordo com situações especificas, 81% dos participantes estão nesse grupo, comparados com 50% no

estudo de Westin.

Participantes que possuem uma nota maior que 90 foram classificados como “fundamentalistas”, o que significa que eles demonstraram alto nível de preocupação com todas as situações envolvendo sua privacidade.

Grupo	Westin	Este estudo
Fundamentalistas	25%	3%
Pragmáticos	50%	81%
Despreocupados	25%	16%

Tabela 4 - Comparação de tipologia

Como mostrado na tabela 2, esses resultados mostram diferenças significativas entre consumidores que responderam a este estudo e consumidores no estudo de Westin (Westin, 2003), com mais participantes no estudo atual compondo a categoria dos pragmáticos. Considerando esses dados, a tipologia de Westin foi revisada para segmentar os participantes em quatro categorias distintas, a categoria dos pragmáticos foi dividida em duas: Aqueles que a nota varia entre 31 e 60, e os que a nota varia entre 61 e 89. Essas segmentações refletem duas diferentes segmentações do pragmatismo. Primeiro existe um grupo de participantes que possuem um nível de preocupação pouco maior que o grupo dos despreocupados, porem que no geral possuem um nível moderado. Em segundo lugar existe um grupo de participantes com um nível de preocupação moderadamente maior, porém não tanto quanto os fundamentalistas. Essa categorização resulta em uma tipologia que consiste de quatro grupos distintos de consumidores virtuais, baseando-se em seu nível de preocupação com a privacidade. Os quatro grupos foram chamados de despreocupados, discretos, cautelosos e alarmados. Uma breve descrição de cada grupo é dada a seguir.

- Despreocupado

  Participantes com uma nota total de 30 ou menos (media total de 20.53), esses indivíduos demonstraram mínima preocupação com a maioria das 15 situações e representaram 16% do total de participantes. A única situação em que esse grupo se sente altamente preocupado é quando são pedidos para informar dados como números de documentos, uma situação que demostrou ser de alta preocupação com todos os participantes.

- Discretos

  Participantes com uma nota entre 31 e 60 (media total de 46.65, significativamente maior que o grupo dos despreocupados). Indivíduos nesse grupo sentem um nível de preocupação baixo a moderado com a maioria das situações, duas das situações causaram um nível maior de preocupação: além da situação dos números de documentos apresentada anteriormente , esses usuários também se preocupam a respeito do uso de informações por outras organizações além das quais ele realizou algum tipo de cadastro ou transação. Esse grupo representa 38% do total de participantes.

- Cautelosos

  Participantes com uma nota total de preocupação entre 61 e 89 (media total de 72.84, significativamente maior que a dos discretos). Esse grupo sentiu um nível moderado de preocupação na maioria das situações. Três das situações causaram um alto nível de preocupação: Em adição as duas mencionadas anteriormente, este grupo também se preocupou com práticas clandestinas de coleta de dados. Esse grupo representa 43% dos participantes.

- Alarmados

  Participantes com uma nota maior que 90 (media total de 96.26, significativamente maior que os cautelosos). Esse grupo é altamente preocupado com sua privacidade em todas as situações. Esse grupo representa 3% dos participantes.

As medias totais das notas de cada grupo variam significativamente entre si, dessa forma, é possível abordar a segunda questão da pesquisa, para analisar se esses grupos mostram alguma diferença baseada na demografia e uso da internet.

6.4 DIFERENÇA ENTRE GRUPOS

6.4.1 DEMOGRAFIA

A tabela 3 mostra os perfis demográficos de cada um dos quatro grupos. Não há diferenças significativas entre os grupos levando em conta o gênero, em todos os grupos o perfil do participante consiste de uma maioria masculina. Entretanto existem diferenças em termos de idade e escolaridade, essa relação é ilustrada na figura 1.

Em relação as diferentes faixas etárias entre os grupos, é aparente a diferença. Os usuários despreocupados e os alarmados, são relativamente mais velhos que os discretos e cautelosos. Mais de 40% dos participantes nos grupos dos despreocupados e alarmados tem mais de 45 anos de idade, onde cerca de 30% dos discretos e cautelosos tem mais de 45 anos.

Levando em conta a escolaridade, os dois grupos com notas menores de preocupação com a privacidade tendem a ter um grau de escolaridade menor que os outros dois grupos com um nível maior de preocupação. Enquanto 15% dos dois grupos menos preocupados possuem mestrado ou doutorado, cerca de 25% dos usuários pertencentes aos grupos mais preocupados possuem o mesmo nível mais elevado de escolaridade. Os dados sugerem que indivíduos com um maior grau de escolaridade se preocupam mais com sua privacidade online que pessoas com menor escolaridade.

		Despreocupados	**Discretos**	**Cautelosos**	**Alarmados**
Preocupação total		20,53	46,65	72,84	96,26
Gênero	**Masculino**	71%	76%	66%	67%

	Feminino	29%	24%	34%	33%
Idade	**18 - 24**	21%	21%	11%	12%
	25 -34	18%	26%	29%	17%
	35 - 44	19%	24%	30%	21%
	45 - 54	29%	23%	19%	33%
	55 - 64	9%	5%	9%	4%
	65+	5%	2%	3%	13%
Escolaridade	**Superior ou menor**	85%	80%	67%	67%
	Mestrado ou maior	15%	20%	33%	33%

Tabela 5 - Comparação de grupos: diferenças demográficas

Figura 2 - Tipologia de preocupação com a privacidade de usuários

6.4.2 USO DA INTERNET E AÇÕES

A tabela 4 mostra um resumo do perfil de uso da internet entre os quatro grupos. Não há diferenças significantes nas categorias mais básicas de uso, Participantes de todos os grupos afirmaram estar usando a internet por entre 15 e 17 anos e cerca de 75% de seu tempo online é em casa, a maioria dos participantes em todos os grupos afirmam que utilizam a internet regularmente e verificam seus e-mails várias vezes ao dia, menos de 25% dos participantes adotam uma identidade falsa na

internet e a maioria dos participantes em todos os grupos recebem e-mails não solicitados.

Os participantes nos quatro grupos também foram semelhantes em seu comportamento a respeito de diferentes ações online: Os participantes leem e-mails não solicitado cerca de 50% das vezes que os recebem e apenas ocasionalmente se desinscrevem de listas de e-mails, no entanto algumas diferenças em ações entre os grupos foram observadas.

Considerando os usuários que requerem a desinscrição de listas de e-mails, os usuários “alarmados” requerem a remoção de seus nomes de listas cerca de metade das vezes que eles têm a oportunidade (média de 4.04). Os outros grupos informam uma frequência significativamente menor na mesma ação.

Os participantes raramente reclamam com o remetente de e-mails não solicitados, entretanto, membros do grupo mais preocupado informam uma quantidade significativamente maior de reclamações do que os outros três grupos (média do grupo “alarmados” de 2.43). Os membros do grupo dos cautelosos informaram que reclamaram menos frequentemente (média de 1.65) que o grupo dos alarmados. Isso pode sugerir que níveis maiores de preocupação podem levar a adoção de medidas mais “agressivas” na internet, apesar dessa descoberta possuir menor chances, em média, de acontecer.

Os participantes menos preocupados (despreocupados e discretos) se registram em cerca de 50% dos sites que possuem a possibilidade de registro (média de 3.38 e 3.40 respectivamente). Essa frequência de registros é significativamente maior do que os grupos mais preocupados, que informaram se registrar menos da metade das vezes (média de 2.95 para os cautelosos e 2.38 para os alarmados). Isso sugere que o nível de preocupação com a privacidade pode afetar a possibilidade de usuários informar seus dados no processo de registro em diferentes sites.

Os usuários despreocupados informam dados incompletos menos frequentemente que os outros três grupos (média de 3.18 para os usuários despreocupados, a menor média para os outros grupos foi de 3.58 para os usuários discretos). Prover

informações incompletas é uma forma de proteger a privacidade enquanto ainda pode participar de atividades online, o que talvez seja a razão para que quanto mais preocupado com a privacidade se é, mais os usuários decidem omitir determinadas informações.

Os usuários alarmados e os cautelosos informam dados incorretos mais frequentemente que os despreocupados e discretos. Os cautelosos e os alarmados informam dados incorretos ocasionalmente (média de 2.30 e 3.05 respectivamente), enquanto as notas medias dos usuários despreocupados e dos discretos sugerem que esses grupos raramente o fazem (a média de ambos os grupos foram de 2 ou menos). Assim como na última descoberta, informar dados incorretos, é uma forma de participar de atividades online enquanto protege sua privacidade.

		Despreocupados	Discretos	Cautelosos	Alarmados
Preocupação Total		20,53	46,65	72,84	96,26
Anos na internet		16,12	17,16	17,06	15,38
Quantidade de tempo online por local	**Casa**	76%	73%	74%	72%
	Trabalho	19%	20%	23%	23%
	Escola	3%	6%	2%	4%
	Outro	2%	1%	1%	1%
Recebeu e-mail não solicitado		88%	90%	91%	96%
Verifica e-mail diversas vezes no dia		67%	70%	61%	58%
Adota uma identidade alternativa na internet		29%	27%	30%	27%
Frequência de:					
	Leitura de e-mails não solicitados	3,8	3,59	3,46	2,72

Desinscrição de listas de e-mails	2,41	2,62	2,97	4,04
Reclamar com o remetente de e-mails não solicitados	1,55	1,34	1,65	2,43
Registros em sites	3,38	3,4	2,95	2,43
Informar dados incompletos ao se cadastrar	3,18	3,58	3,85	3,94
Informar dados incorretos ao se cadastrar	2	1,95	2,3	3,05

Tabela 6 - Comparação de grupos: Uso da internet

6.4.3 RESUMO

De acordo com essas descobertas que indicam que cada um dos quatro grupos exibe características únicas, é aparente que a tipologia de Westin é limitada para categorizar usuários da internet. Considerando que esse estudo usou 15 medidas para analisar preocupação com a privacidade, não é nada surpreendente que uma variância maior entre os usuários seja observada. Essa pesquisa sugere que duas variáveis chave de demografia aparecem distintas para os grupos, ou seja, essa tipologia sugere que a orientação de indivíduos a respeito da privacidade pode ser influenciada pelas suas faixas etárias e pelo seu nível de escolaridade. Para brevemente resumir as diferenças entre os quatro grupos:

- Usuários despreocupados exibem pouca preocupação com sua privacidade na internet. Eles são relativamente mais velhos que a média e tem um grau de escolaridade menor. Os despreocupados raramente reclamam dos remetentes de e-mails não solicitados e, em média, se registram em sites

metade das vezes em que existe essa possibilidade, eles raramente informam dados incorretos.

- Os usuários discretos, em média se preocupam pouco com a privacidade, entretanto algumas situações podem fazer com que eles tenham níveis maiores de preocupação. Eles são em relativamente mais novos que a média e tendem a ter um nível de escolaridade menor. Em termos de comportamentos, eles são similares aos usuários despreocupados, são os menos prováveis de enviar reclamações, além de se registarem em cerca de metade dos sites que encontram, porém são mais propensos a informar dados incompletos ao se cadastrar em sites.

- Os usuários cautelosos tem um nível moderado de preocupação com sua privacidade em várias situações, o que faz com que eles experienciem preocupação maior que a média com a privacidade. Esses usuários tendem a ser mais jovens e tem um nível de escolaridade mais alto, eles reclamam com mais frequência sobre e-mails não solicitados, eles se registram apenas ocasionalmente em sites e possuem maior chance de informar dados incompletos ou incorretos ao se cadastrar.

- Usuários alarmados são altamente preocupados com sua privacidade na internet. Eles são mais velhos e possuem em média um nível de escolaridade maior, eles são os mais prováveis a reclamar com as organizações. Eles raramente se registram em sites, porem quando o fazem são mais propensos a informar dados incompletos e incorretos.

6.4.4 CONCLUSÃO DA PESQUISA

Este estudo explorou as diferenças entre usuários no que diz respeito sua preocupação pela privacidade na internet, foi utilizada uma tipologia estabelecida e

analisado se os usuários se encaixavam nela. A tipologia foi expandida para levar em consideração o contexto do ambiente virtual da internet.

Como um estudo exploratório, sofreu de algumas limitações, como por exemplo o método de distribuição da pesquisa que não atingiu um número de participantes tão grande quanto poderia, além disso, dado o tópico da pesquisa, é possível que um número de possíveis participantes que sejam muito preocupados com sua privacidade não tenham a respondido. Portanto a categoria dos usuários “alarmados” pode ter não ter sido totalmente representada.

Outras descobertas dessa pesquisa sugerem outras áreas para futuros estudos. Por exemplo, uma futura pesquisa poderia aprofundar seus estudos nessas quatro categorias para entender mais suas motivações. A partir desses dados, é aparente que a categoria dos usuários alarmados é a única que consistentemente toma medidas para proteger sua privacidade.

7. CENÁRIO IDEAL

Depois de analisar algumas ferramentas e o conceito de privacidade, é possível que junto de um certo padrão de comportamento na internet, ajude com que os usuários consigam atingir um nível mais avançado de privacidade, garantindo assim seus direitos e liberdade.

7.1 FERRAMENTAS

O uso de redes sociais, é um grande fator a se considerar hoje em dia. Considerando sua natureza gratuita para o usuário final, fica evidente que a real mercadoria em circulação pela rede é a informação gerada pelo usuário, assim como, nome, sexo, idade, localização, preferencias pessoais, redes de amigos e etc. Com todas essas informações, é possível criar uma grande rede de informação para ser usada a favor da rede, como principalmente o uso de propaganda direcionada para cada individuo especifico, levando em conta seu perfil.

7.1.1 TOR BROWSER E EXTENSÕES

O navegador disponibilizado pelo Tor Project, possui diversas extensões (ferramentas independentes do navegador) embutidas que podem ajudar nas situações mencionadas anteriormente no caso da coleta de dados passiva pelos websites ou terceiros. Ele também só armazena dados de navegação por seção, ou seja, sempre que o navegador for reiniciado todos os dados gerados na seção anterior são apagados, assim como cookies.

Uma das extensões disponíveis no navegador Tor é o HTTPS-Everywhere, que criptografa toda a comunicação na maioria dos websites. Muitos sites na internet oferecem um suporte limitado a criptografia através do https, mas a tornam difíceis de utilizar, por exemplo, eles podem por padrão encaminhar uma solicitação não criptografada através de http simples, ou colocar em páginas que estão criptografadas, links que levam a paginas menos seguras. Essa extensão corrige esses problemas reescrevendo requisições para os sites utilizando https.

Outra extensão disponível é o NoScript, um software grátis disponível para navegadores baseados no Mozilla. Por padrão, o NoScript bloqueia conteúdos ativos (executáveis) em websites como por exemplo JavaScript, WebGL, flash e outros. Devido a muitos ataques envolvendo navegadores web necessitarem conteúdo ativo que o navegador normalmente executa por padrão, desabilitar esse tipo de conteúdo por padrão e utilizando-o apenas o mínimo do que é necessário, reduz a chance de exploração de vulnerabilidades além de negar alguns tipos de rastreios online.

7.1.2 SERVIÇOS DE VPN

Outro modo de minimizar a exposição de nossos dados na internet é o uso de um serviço de vpn. Atualmente existem dezenas de diferentes serviços a disposição do público, apesar de muitos serem pagos, existem alternativas gratuitas.

Ao utilizar um desses serviços o usuário, além de conseguir uma conexão mais segura como já mencionado anteriormente, é possível atravessar certos bloqueios e censura, assim como conteúdo restrito a determinadas regiões e possíveis bloqueios instaurados por agências governamentais.

7.2 CUMPRIMENTO DA LEI

Uma situação que não pode ser ignorada num cenário ideal de privacidade é o cumprimento da lei por empresas que armazenam ou manipulam informação de usuários. Para que esse cenário seja o mais ideal possível é necessário que empresas adotem as medidas estipuladas pela lei de forma a melhor proteger nossos dados, além de nos fornecer informação clara e precisa de como e porque nossos dados vão ser utilizados, além de, claramente pedir pelo consentimento do usuário.

7.3 COMPORTAMENTO DO USUÁRIO

Apenas a utilização de todos os serviços mencionados não é o suficiente para garantir toda a privacidade e o anonimato desejado pelo usuário, portanto, para tal, é necessária a adoção de certos comportamentos ao navegar pela internet para que o cenário possa ser atingido.

Como evidenciado pela pesquisa com o público, um percentual considerável dos usuários se preocupa com sua privacidade, portanto algumas ações individuais podem ajudar a garantir maior privacidade. Algumas das ações podem ser a omissão ou alteração de dados que considere mais pessoais em redes sociais, denúncia sobre o possível uso indevido de dados para os órgãos competentes (com a entrada em vigor da LGPD) além de verificar qual tipo de site é realmente necessário se efetuar um cadastro.

Se atentar a que tipo de rede se está utilizando para conectar na internet é outro fator importante, pois sempre é possível que terceiros tenham acesso ao trafego de informação em redes públicas ou até mesmo privadas. Portanto o ideal é evitar acessar informação sensível, como por exemplo, contas de banco, em redes que não confie.

8. CONSIDERAÇÕES FINAIS

O desenvolvimento do presente estudo possibilitou uma análise do porque a privacidade ou o anonimato são importantes em um contexto virtual, para, principalmente, garantir liberdades individuais e coletivas neste meio.

Podemos também entender melhor o funcionamento de ferramentas como VPNs e a rede Tor e como elas podem ajudar a melhorar o cenário de privacidade na internet.

Um dos temas abordados foi o da Lei geral de proteção dos dados (LGPD) que tem como objetivo fazer com que empresas e organizações que atuam na internet e/ou armazenem e manipulem dados de usuários, tenham mais empenho em manter esses dados seguros, além de “devolver” para o usuário o controle sobre seus próprios dados, para que ele decida a finalidade dos mesmos.

A pesquisa desenvolvida com o público, conseguiu gerar resultados que mostram qual é o perfil do usuário da internet no que diz respeito sua preocupação com a privacidade, dividindo-os em quatro grupos distintos, o que ajudou na melhor visualização dos dados, e que tipo de comportamento básicos são adotados por eles, indicando que uma quantidade considerável de indivíduos, se preocupa com sua privacidade.

Portanto, com a conclusão desse trabalho, é possível que essa porcentagem de usuários que se preocupam com a privacidade possa entender melhor como seus dados são utilizados, além de conhecer formas de garantir sua própria privacidade e, possivelmente, para os que foram considerados “despreocupados” este trabalho pode ser útil para entender melhor o porque talvez seja melhor se preocupar mais com alguns aspectos da internet.

REFERÊNCIAS

BUTCHER, Isabel. **4,55 bilhões de dados em todo mundo foram roubados, perdidos ou comprometidos, diz Gemalto**. Disponível em: <https://www.mobiletime.com.br/noticias/09/10/2018/455-bilhoes-de-dados-em-todo-mundo-foram-roubados-perdidos-ou-comprometidos-diz-gemalto/>. Acesso em: 31 out. 2019.

CHIN, Liou Kl. **Rede Privada Virtual - VPN**, 1998. Disponível em: <https://memoria.rnp.br/newsgen/9811/vpn.html>. Acesso em: 30 mar. 2020.

DINGLEDINE, Roger; MATHEWSON, Nick; MURDOCH, Steven; SYVERSON, Paul. Tor: The Second-Generation Onion Router (2014 DRAFT v1).

IETF Tools. Internet Key Exchange Protocol Version 2 (IKEv2). Disponível em: < https://tools.ietf.org/html/rfc7296>. Acesso em: 20 jun. 2020.

LEITE, Henrique Specian. **A Importância da Privacidade na Internet.** 2016. 61 f. TCC (Graduação) – Tecnologia em Análise e Desenvolvimento de Sistemas, Departamento de Tecnologia da Informação, Faculdade de Tecnologia de São Paulo, São Paulo, 2016.

LGPD. LGPD Brasil, 2020. Disponível em: <https://www.lgpdbrasil.com.br>. Acesso em: 20 fev. 2020.

MILNE, George R. Consumer Participation in Mailing Lists: A Field Experiment. Journal of Public Policy & Marketing – Volume 16. Amherst, Massachusetts, USA, 1997. p.298-309.

MILNE, George R; GORDON, Marry E. Direct mail privacy-efficiency trade-offs within an implied social contract framework. Journal of Public Policy & Marketing – Volume 16. Amherst, Massachusetts, USA, 1993. p.206-2015.

NOWAK, Glen J; PHELPS, Joseph. Direct marketing and the use of individual-level consumer information: Determining how and when “privacy” matters. Journal of Direct Marketing – Volume 11. Nova Iorque, Nova Iorque, USA, 1995. p.46-60.

PLANALTO. Planalto, 2020. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 20 fev. 2020.

PRIVACY TOOLS. Privacy tools, 2019. Disponível em: <https://www.privacytools.io/>. Acesso em: 31 de outubro, 2019.

TOR. Tor Project, 2019. Disponível em: <https://www.torproject.org/>. Acesso em: 31 out. 2019.

TOR Metrics. Tor Project, 2020. Disponível em: < https://metrics.torproject.org/>. Acesso em: 20 jun. 2020.

WESTIN, Alan F. Privacy and freedom. Nova Iorque: Ig Publishing,1967

WESTIN, Alan F. Social and Political Dimensions of Privacy. Journal of Social Issues – Volume 11. Nova Iorque, Nova Iorque, USA, 2003. p.431-453.