PRIVACIDADE E SEGURANÇA DE DADOS DE USUÁRIOS: ANÁLISE DO CASO CADASTRO POSITIVO

PRIVACY AND SECURITY OF USER DATA: ANALYSIS OF THE CADASTRO POSITIVO

Bruna Logatti[*]
Cristina Cibeli Vidotti Ivo de Medeiros[**]

RESUMO

O trabalho desenvolveu um estudo sobre as questões da privacidade e segurança de dados disponibilizados pelos usuários da internet. Com base na pesquisa, decidiu-se restringir a um estudo de caso referente ao Cadastro Positivo do Serasa. Criado pela Lei 12414 de 2011, o Cadastro Positivo consiste de um banco de dados que reúne uma série de informações sobre os consumidores. Em abril, a Lei 12414 foi alterada, estabelecendo a inclusão de todos consumidores brasileiros. Assim, o estudo estabeleceu 4 objetivos, focando na legislação, nos órgãos de defesa dos direitos dos consumidores, nos consumidores brasileiros e nos profissionais da área. Para a coleta de dados foram feitas entrevistas, questionários, conversas informais etc. Como resultado obteve-se que com as mudanças na Lei 12414/2011, a preservação da privacidade e a segurança dos dados dos consumidores piorou. Em relação à questão do Cadastro Positivo do consumidor deve haver uma análise de cada caso, se existir a prioridade em manter a privacidade e segurança, recomenda-se descadastrar. Porém, existirá uma série de efeitos negativos sobre futuras compras.

Palavras-chave: Privacidade e Segurança de Dados. Coleta de Dados. Cadastro Positivo.

ABSTRACT

This paper studied the privacy and data security issues of internet users. Based on the research and the large amount of information, it was decided to restrict the study, addopting a case of study regarding Serasa's “Cadastro Positivo” (positive record). Created by Law 12414 of 2011, the positive register consists of a database that gathers a series of information about consumers. In April, Law 12414 was amended, establishing the inclusion of all Brazilian consumers. Thus, the study established 4 objectives, focusing on legislation, in the defense of consumer rights, the consumers and professionals. To collect data, interviews, questionnaires and conversations were made. As results of the study about changes in Law 12414/2011 there is: the lost of privacy and data security of the consumers, as for the issue of “Cadastro Positivo”, there should be an analysis of each case, if there is a priority in maintaining privacy and security, it is

[*] Graduada em Engenharia de Computação e Mestre em Engenharia Urbana – FIAR, Faculdades Integradas de Araraquara. bru.logatti@gmail.com
[**] Graduada em Análise de Sistemas/ Mestre em Ciências da Computação – FIAR, Faculdades Integradas de Araraquara.

recommended to unsubscribe. However, there will be a number of negative effects on upcoming purchases of the consumer.

Keywords: Privacy and Data Security. Data Collection. “Cadastro Positivo”.

Introdução

Desde 1948, o ser humano busca definir a privacidade e segurança de dados pessoais. No entanto, naquela época, não existiam tantas ferramentas para coleta de dados e essas ferramentas não eram dispositivos que ficam diariamente nas mãos dos homens. Com a chamada “revolução digital”, o surgimento de dispositivos elétrico-eletrônicos, que estão constantemente conectados à *World Wide Web*, era somente uma questão de tempo, assim como discussões sobre a nova privacidade e segurança dos usuários da *internet* (ONU, 1948).

Com base nesse assunto, esse trabalho objetivou desenvolver um estudo sobre o que é privacidade e segurança no âmbito digital, como ela é definida, quais são as legislações existentes sobre esse assunto. No entanto, é necessário o questionamento de que se a segurança digital realmente protege os dados e assim a privacidade de milhões de usuários da internet. Além desses aspectos, também se procurou mostrar o que existe de mais novo em tecnologias no que diz respeito à coleta, ao tratamento e à segurança de dados. Mas a questão mais relevante sobre esse assunto é o que as grandes empresas fazem com os dados adquiridos.

Tendo como base tantos questionamentos e um número crescente de empresas que utilizam os dados de seus usuários, decidiu-se desenvolver um estudo de caso sobre uma dessas empresas: o Cadastro Positivo do Serasa. Esse cadastro é um banco de dados que existe desde 2011 (Lei 12414), entretanto foi em abril de 2019 que ele sofreu sua maior mudança: a inclusão de todos os consumidores do Brasil.

A realização desse estudo de caso buscou descobrir o que será feito com os dados coletados dos consumidores, como esses dados poderão ser usados, e como poderão afetar a privacidade e segurança dos mesmos. Para a obtenção de resultados, estabeleceu-se um objetivo principal de pesquisa, que englobou quatro grandes tópicos:

1. determinar como as legislações que dizem respeito à preservação da privacidade e da segurança de dados dos consumidores trabalham a favor dos consumidores;

2. consultar como o órgão de defesa dos direitos dos consumidores (PROCON) se posiciona à respeito da mudança da Lei nº 12.414, de 9 de junho de 2011;
3. verificar se os consumidores têm conhecimento sobre as mudanças da Lei nº 12.414, de 9 de junho de 2011;
4. abordar as possíveis vantagens da alteração no Cadastro Positivo e como ele opera.

Assim, foram aplicadas diferentes técnicas de coleta de dados, sendo elas: entrevista, questionário, participação em palestras e conversas informais. Após a coleta das informações, fez-se análise e discussão a respeito da privacidade e segurança dos consumidores inseridos no Cadastro Positivo.

Síntese Bibliográfica

Privacidade e Segurança

Conforme Ferreira (2008, p. 654), a privacidade pode ser definida em apenas uma palavra "intimidade". Esta, por sua vez, é definida como "vida íntima, particular" (FERREIRA, 2008, p. 487). O artigo 12 da Declaração Universal dos Direitos Humanos (1948) diz que: "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei".

No Brasil, o direito à privacidade é estabelecido por diferentes meios e legislações, sendo os principais a Constituição de 1988, a Lei Nº 10.406, de 10 de janeiro de 2002 (Código Civil) e o Decreto Nº 592, de 6 de Julho de 1992 (Pacto Internacional sobre Direito Civis e Políticos).

No entanto, um fator que não era previsto em 1948 é o recolhimento de dados por empresas e governos, após o desenvolvimento da chamada "Revolução Digital", através da qual o ser humano vive constantemente conectado e vigiado, através de computadores, celulares, câmeras de segurança, *gadgets (smartwatches, smartbands, etc.)*, *wifi*, entre outros. (ONUBR, 2018).

A privacidade é indispensável para o desenvolvimento, tanto da personalidade humana, quanto da dignidade. Ela garante a segurança da vida privada diante de interferências não autorizadas, ou seja, até que grau o indivíduo deseja interagir com o

mundo. Ela é responsável por delimitar fronteiras de acesso aos corpos, coisas, lugares, dados, informações e comunicações do homem (ONUBR, 2018).

Entretanto, a chamada privacidade digital ainda é vista como um conceito abstrato. Sendo constantemente quebrada por governos, utilizando os argumentos de segurança nacional, e por empresas, quando são aceitos seus termos em meio a uma compra ou um serviço online. Mas a sociedade, na maior parte das vezes, não está ciente das informações e dados que está disponibilizando e para quem. Esse fato faz com que a alegação: "caso você tenha ganhado algo de graça no mundo digital, significa que você é o produto", torne-se válida (ONUBR, 2018).

Tendo em vista esse cenário, no Brasil, existe um grande desenvolvimento no que diz respeito à legislação que garanta a privacidade digital, como o Marco Civil da Internet (2014) e a Lei Geral de Proteção de Dados (2018), porém é necessário um estudo para avaliar até que ponto esses são realmente efetivos para a segurança dos dados de usuários da internet.

Marco Civil da Internet – Lei 12965/2014

O Marco Civil da Internet, implantado por meio da Lei 12.965, de 23 de abril de 2014, estabeleceu garantias, direitos, deveres e princípios para o uso da Internet no Brasil. De modo geral, ele tenta disciplinar o uso da internet no Brasil, tendo em vista os princípios da garantia da liberdade de expressão, da proteção da privacidade, da proteção de dados pessoais, da preservação e garantia da neutralidade da rede e da preservação da natureza participativa da rede (BRASIL, 2014).

Dentre esses princípios se destaca o direito à privacidade, que se encontra nos incisos I,II,II, VII e VII do art 7º. Esse direito seria, do ponto de vista do direito civil, impedir acesso de terceiros a informações pessoais e direito de se isolar do contato humano, incluindo itens como: inviolabilidade da intimidade e da vida privada, preservação do sigilo nas comunicações privadas pela rede, não fornecimento de informações dos usuários sem prévio consentimento para terceiros e informar e justificar ao usuário quando houver coleta de dados sobre si (TOMASEVICIUS FILHO, 2016).

Tomasevicius Filho (2016) ainda destaca o artigo 14, que diz respeito a provedores. Estes não podem guardar registros de acesso a aplicações da internet sem o prévio consentimento do usuário, muito menos guardar dados pessoais desnecessários à finalidade para qual o usuário consentiu.

Entretanto, tem-se um fator determinante para que o sucesso do Marco Civil da Internet seja efetivo: outros países devem adotar uma legislação similar, senão idêntica, já que a própria estrutura da internet faz com que existam violações dos direitos das pessoas, independentemente da localização mundial, ou seja, mesmo com uma Lei assegurando os direitos civis dos brasileiros na Internet, esses podem ter seus direitos violados em qualquer outra parte do mundo, a qualquer hora e por qualquer outro usuário (TOMASEVICIUS FILHO, 2016).

Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados (LGPD), conhecida como Lei nº 13.709, de 14 de agosto de 2018, alterou o Marco Civil da Internet e aprofundou a proteção de dados pessoais na Internet. De acordo com o artigo 2º da LGPD, a proteção de dados pessoais tem como fundamentos: respeito à privacidade, autodeterminação informativa, liberdade de expressão, de informação, de comunicação e de opinião, inviolabilidade da intimidade, da honra e da imagem e os direitos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania pelas pessoas naturais (BRASIL, 2018).

Monteiro (2018) aponta que a lei transplanta o sistema setorial de proteção de dados para um geral. Baseada na GDPR europeia, também determina os dois direitos dos usuários, sendo eles: o direito de explicação e de revisão. A lei buscou garantir às pessoas controle sobre suas informações e, ao mesmo tempo, desenvolver um ambiente de desenvolvimento econômico e tecnológico.

Dentre seus itens, o mais importante é o direito de transparência aos titulares dos dados, esses podem ter conhecimento sobre a realização do tratamento em seus dados e seus respectivos agentes, com o objetivo de tornar os algoritmos responsáveis menos obscuros e opacos, garantindo aos usuários informações claras, precisas e de fácil acesso sobre qualquer processo, sistema, rede etc., dos quais possa participar (MONTEIRO, 2018).

A Segurança de Dados na Internet

Os dados que são disponibilizados na internet passaram a se tornar parte integrante da vida do usuário, portanto uma parcela da vida do ser humano passou a ser controlada por meio de algoritmos. Os algoritmos são sequências pré-definidas de instruções

automatizadas que, com base nos dados disponíveis (pessoais e não pessoais), conseguem gerar respostas que sujeitam o usuário à determinada ação (MONTEIRO, 2018).

Com a revolução digital, sistemas mais complexos começaram a surgir e utilizam, principalmente, o aprendizado de máquina e a inteligência artificial como base. Sua principal característica é a natureza adaptativa, chega-se a um ponto em que é impossível determinar os resultados finais e a lógica desses sistemas. Tal opacidade dificulta que o usuário entenda e verifique como seus dados pessoais são tratados, ou seja, se é de uma forma legítima, adequada e proporcional (MONTEIRO, 2018).

Tal cenário faz com que as leis de proteção de dados se tornem imprescindíveis para a segurança dos dados e, consequentemente, da vida do ser humano na internet. Garantindo que seus direitos fundamentais sejam respeitados. Conforme Monteiro (2018), são eles:

- direito à saúde;
- direito à educação;
- direito ao pleno emprego;
- direito à informação;
- direito à liberdade;
- direito à cidadania.

Tendo em vista tais pontos, deve ser verificado como as principais empresas desenvolvedoras de *softwares*, redes sociais, computadores, produtos eletrônicos, entre outros, utilizam os dados pessoais fornecidos pelos seus usuários a seu favor.

Google

O Google disponibiliza uma série de serviços, *hardwares* e sistemas operacionais para qualquer pessoa que tenha interesse. Dentre esses, destaca-se a Conta do Google responsável por gerenciar conteúdo, como *e-mails*, fotos, documentos, vídeos, ver resultados de pesquisa mais relevantes e aplicativos, caso o usuário tenha um dispositivo *Android*. É possível também usar serviços do Google sem criar uma conta, como pesquisar no Google ou assistir a vídeos (GOOGLE, 2019).

Em sua Política de Privacidade, o Google informa que coleta uma série de informações básicas, como o idioma; ou complexas, como anúncios que o usuário considera mais útil, as pessoas *on-line* mais importantes, os vídeos mais curtidos. As

informações coletadas pelo Google e como essas informações são usadas dependem do uso dos serviços e do gerenciamento do controle de privacidade (GOOGLE, 2019).

Quando não conectado a uma Conta do Google, existe o armazenamento das informações com identificadores exclusivos vinculados ao navegador, aplicativo ou dispositivo usado. Quando conectado, essas informações são coletadas e armazenadas na Conta do Google e são tratadas como informações pessoais (GOOGLE, 2019).

Ao criar uma Conta do Google, são fornecidas informações pessoais como: nome e senha. O usuário pode optar por adicionar número de telefone ou informações de pagamento. Porém, a empresa coleta todo o conteúdo criado, aquele que se faz *upload* e o recebido de outras pessoas ao usar os serviços. Isso inclui e-mails enviados e recebidos, fotos e vídeos salvos, documentos e planilhas criados e comentários (GOOGLE, 2019).

Coletam-se informações sobre os *apps*, navegadores e dispositivos utilizados para acessar os serviços. As informações coletadas incluem identificadores exclusivos, tipo e configurações de navegador, tipo e configurações de dispositivo, sistema operacional, informações de rede móvel, incluindo nome e número de telefone da operadora e número da versão do aplicativo. Informações sobre a interação de *apps*, navegadores e dispositivos com os serviços Google são coletadas, incluindo endereço IP, relatórios de erros, atividade do sistema, data, hora e URL referenciador da sua solicitação (GOOGLE, 2019).

Além disso, informações de atividades também são armazenadas, como: termos pesquisados, vídeos assistidos, visualizações e interações com conteúdo e anúncios, informações de voz e áudio dos recursos de áudio, atividade de compra, pessoas com quem se comunica ou compartilha conteúdo, atividades em *sites* e *apps* de terceiros que usam os serviços Google, histórico de navegação. Caso seja usado o serviço para fazer e receber chamadas ou enviar e receber mensagens, pode-se coletar informações de registro de telefonia, como o número do chamador, número do receptor, números encaminhados, horário e data de chamadas e mensagens, duração das chamadas, informações de roteamento e tipos de chamadas (GOOGLE, 2019).

Por fim, também são armazenadas informações sobre localização, ela pode ser determinada com vários graus de precisão por meio de GPS, endereço IP, dados do sensor do dispositivo, informações de itens próximos do dispositivo, como pontos de acesso *Wi-Fi*, torres de celular e dispositivos com *Bluetooth* ativado (GOOGLE, 2019).

Em algumas circunstâncias, o Google também coleta informações em fontes de acesso público, de parceiros confiáveis e de anunciantes para fornecer serviços de

publicidade e pesquisa em nome deles. Utilizam-se diversas tecnologias para coletar e armazenar informações, incluindo *cookies*, *tags* de *pixel*, armazenamento local como armazenamento do navegador da *Web* ou *caches* de dados de aplicativos, bancos de dados e registros do servidor (GOOGLE, 2019).

Conseguindo dois bilhões de usuários em dez anos por meio de seu sistema *Android* (LIMA, 2018), a principal fonte de informações do Google são os dados coletados nos dispositivos móveis que apresentam esse sistema. Entretanto, existe outra grande empresa que apresenta um grande número de usuários de um mesmo sistema operacional (*Windows*) e que conseguiu ultrapassar o valor de mercado do Google no início de 2018 (US$ 753 bilhões contra US$ 739 bilhões), a Microsoft (CANALES, 2018).

Microsoft

A Microsoft oferece uma ampla variedade de produtos, incluindo sites, aplicativos, *software*, servidores, dispositivos e serviço. A Microsoft coleta dados, por meio de interações com o usuário e por meio de seus produtos. Alguns desses dados são fornecidos diretamente, enquanto outros são obtidos ao coletar dados de interações, uso e experiências com os produtos. Os dados coletados dependem do contexto das interações com a Microsoft e as opções escolhidas, como: configurações de privacidade, produtos e recursos usados. Também se obtém dados por meio de terceiros (MICROSOFT, 2019).

Os dados coletados incluem: nome e dados de contato (nome e sobrenome, *email*, endereço, número de telefone e outros dados de contato semelhantes), credenciais (senhas, dicas de senha e informações de segurança semelhantes utilizadas para autenticação e acesso de contas), dados demográficos (idade, sexo, país e idioma preferencial), dados de pagamento (número do meio de pagamento e o código de segurança associado), dados de assinatura e licença (MICROSOFT, 2019).

Já os dados coletados por meio de interações são compostos de: dados de dispositivo e uso (histórico de pagamento e da conta, histórico de navegação, dados de dispositivo, conectividade e configurações, relatórios de erro e dados de desempenho, solução de problemas e dados de ajuda); interesses e favoritos; dados de consumo de conteúdo, pesquisas e comandos; dados de voz; dados de mensagens de texto, escrita a tinta e digitação; imagens; contatos e relações; dados sociais; dados de localização; outros tipos de entradas (MICROSOFT, 2019).

Destaca-se que é coletado todo o conteúdo dos arquivos e comunicações inseridos, carregados, recebidos, criados e controlados dentro do serviço Microsoft, como: áudio, vídeo, texto (digitado, a tinta, ditado ou outra forma), mensagem, *email*, chamada, solicitação de reunião ou *chat*, fotos, imagens, músicas, filmes, *software* e outras mídias ou documentos armazenados, recuperados ou processados de alguma forma em nuvem (MICROSOFT, 2019).

A Microsoft usa os dados coletados de seus usuários para fornecer, melhorar, desenvolver, personalizar e fazer recomendações de produtos, além de anúncios personalizados. Também usa os dados para operar negócios, ou seja, combina dados que coleta de contextos diferentes para oferecer, personalizar serviços (um serviço fornece informações para outro). Contudo, existem proteções tecnológicas e de processos concebidos para impedir determinadas combinações de dados, o que é exigido por lei (MICROSOFT, 2019).

Quando processa dados pessoais, a Microsoft pode fazê-lo com o consentimento do usuário e/ou conforme o necessário para fornecer produtos, operar negócios, cumprir as obrigações contratuais e legais, proteger a segurança de sistemas e de clientes ou atender outros interesses legítimos da Microsoft. Portanto, o processamento de dados engloba as seguintes atividades: (MICROSOFT, 2019).

- fornecer, melhorar, desenvolver e ativar produtos;
- personalização;
- atendimento ao cliente;
- ajudar a proteger e solucionar problemas;
- segurança e atualizações;
- publicidade;
- comércio de transações;
- relatórios e operações de negócios;
- proteger os direitos e a propriedade;
- conformidade jurídica.

Como se pode verificar, são muitos os dados coletados e disponibilizados pelos usuários durante a utilização dos serviços oferecidos pelas grandes empresas. Também se percebe a semelhança entre as políticas de privacidade das diferentes empresas. Além do Google e da Microsoft, destacam-se: *Apple*, a gigante da tecnologia; *Amazon*, responsável por 49,1% de todos os gastos de varejo online nos Estados Unidos (LUNDEN, 2018);

Facebook Inc., fonte de mais de dois bilhões de usuários ativos diariamente na internet (STOUT, 2019).

Essas empresas investem na coleta de dados e desenvolveram dispositivos que permitem a coleta de dados de seus usuários até em suas próprias casas (Google Home e Amazon Alexa). Portanto, é necessário compreender qual a relação entre os dados que são disponibilizados pelos usuários na internet, os dispositivos que são usados no dia-a-dia e como isso pode alterar a privacidade e a convivência do homem em seu meio. Para isso, tem-se a Internet das Coisas (*IoT*).

Internet das Coisas – *Internet of Things (IoT)*

A Internet das Coisas que é composta por três grupos de tecnologias: sensores e dispositivos, inteligência artificial e computação na nuvem. Essas tecnologias norteiam o desenvolvimento da IoT, e podem ser criadas e utilizadas em conjunto ou operarem separadamente, o importante é a interconexão entre os dados e as informações. A IoT visa atender consumidores ao mesmo tempo que explora a digitalização de setores industriais (Figura 1). No que se refere ao consumidor, a IoT é caracterizada pelo uso de dispositivos e sensores conectados à internet (televisores, roteadores, automóveis, *smartphones*, eletrodomésticos, entre outros), sendo intermediada por serviços diversos, principalmente aplicativos. No âmbito comercial e industrial, visa à utilização desses dados com a premissa de cidades inteligentes, monitoramento de pacientes em hospitais, aprimoramento na gestão de recursos energéticos e do setor de saúde (HUREL, LOBATO, 2018).

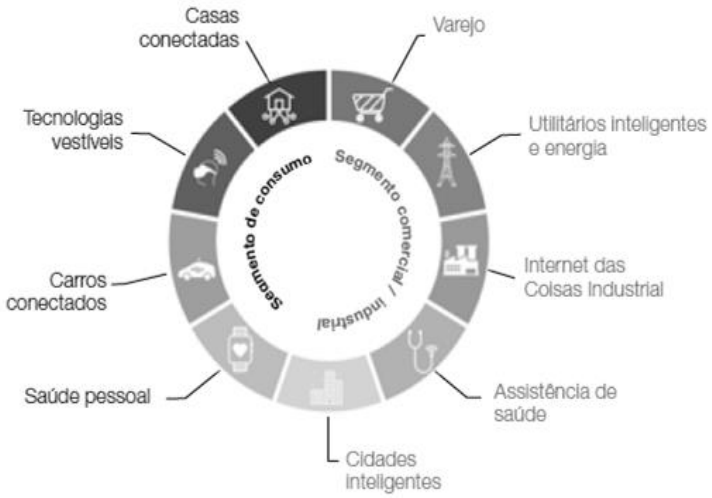

Figura 1 – Panorama do Mercado de IoT.
Fonte: Hurel e Lobato, 2018.

Tendo em vista esses fatos, a IoT é definida, conforme Hurel e Lobato (2018, p. 10) como: "uma rede de sensores que se comunicam e compartilham informações entre si, com o intuito de desempenhar atividades de identificação inteligente, localização, rastreamento, monitoramento e administração de 'coisas' ". Ela é composta por três elementos: o primeiro, chamado de *hardware*, diz respeito aos elementos materiais (dispositivos e sensores). O segundo, denominado *middleware,* é o meio de integração entre dispositivos, sistemas operacionais e diferentes aplicações. Por fim, o terceiro (*software*) é responsável por comunicar a funcionalidade do dispositivo e as suas potenciais operações (HUREL; LOBATO, 2018).

Segundo Hurel e Lobato (2018, p. 7), para a implementação da IoT em larga escala é preciso a habilitação e compreensão:

> - Da confluência entre dados, poder computacional e conectividade, o que compreende IoT, computação na nuvem e Big Data. Essa confluência torna possível o uso ubíquo de sensores e uma redução nos custos de processamento transmissão e armazenamento de dados;
> - Da análise e inteligência de dados, possibilitada por avanços na inteligência artificial e aprendizado de máquina (*machine learning*). Isto favorece processos de digitalização e automação, assim como o desenvolvimento de métodos sofisticados de análise e estatística;
> - Da Interação entre humanos e máquinas (*human to machine*), caracterizada principalmente pelo uso de dispositivos pessoais com interfaces sensíveis ao toque, reconhecimento de gestos e realidade aumentada;

Como destacado nos tópicos de Hurel e Lobato (2018), uma das principais matérias para implementação da IoT é o aprendizado de máquina. Esse é constantemente confundido com a Inteligência Artificial (IA) e é aplicado dentro dos sistemas para uma melhor coleta e análise dos dados. Porém, a complexidade que envolve a *Machine Learning* faz com que muitos de seus processos sejam considerados opacos, sendo esse seu principal problema em relação à segurança e privacidade das informações.

Aprendizado de Máquina (*Machine Learning*)

Desde o início da era tecnológica, pesquisadores sonham em ensinar computadores a raciocinar e tomarem decisões "inteligentes" do mesmo modo que o ser humano faz, ou seja, desenhando generalizações e destilando conceitos de conjuntos de informações complexas sem instruções explícitas (CHIO; FREEMAN, 2018).

O aprendizado de máquina se refere a um aspecto desse objetivo, especificamente aos algoritmos e processos que "aprendem", ou seja, utilizando dados passados e experiências predizer o que ocorrerá no futuro. Em seu núcleo, a *machine learning* é um conjunto de técnicas matemáticas implementadas em sistemas de computadores, que permitem os processos de "mineração" de informações, descoberta de padrões e desenho de inferências a partir de dados (CHIO; FREEMAN, 2018).

Segundo Chio e Freeman (2018), é importante que se compreenda que *machine learning* é um dos componentes da IA, ou seja, ambos se diferem. Como exemplo de distinção entre eles, existe o caso dos carros autônomos. Eles devem classificar imagens observadas como pessoas, carros, árvores; prever a posição e a velocidade de outros carros e determinar até onde as rodas girarão a fim de fazer uma curva. Esses problemas de classificação e previsão são resolvidos usando aprendizado de máquina, e o sistema de autodireção é uma forma de IA. O aprendizado de máquina ajuda na criação de inteligência artificial, mas não é a única maneira de alcançá-la.

Os sistemas de aprendizado de máquina geralmente estão em desacordo com a proteção da privacidade, porque os algoritmos funcionam melhor com dados mais descritivos. Por exemplo, poder acessar um áudio e uma foto de um celular pode dar uma grande quantidade de material para classificar a legitimidade de uma solicitação vinda de um *App* feita por meio de um *login*, mas esse acesso geralmente é considerado uma enorme violação de privacidade (CHIO; FREEMAN, 2018).

Além dos problemas de privacidade relacionados à coleta de dados intrusivos de usuários e terminais, há também a questão do vazamento de informações de modelos de aprendizado de máquina treinados. Alguns modelos de aprendizado de máquina geram saídas que permitem a um observador externo inferir ou reconstruir facilmente: os dados de treinamento que foram incluídos no treinamento do modelo ou os dados de teste que geraram essa saída de previsão. A privacidade diferencial se refere a uma classe de soluções de aprendizado de máquina que visa à preservação da privacidade do usuário, tornando mais difícil para um invasor fazer suposições de alta confiança sobre um fragmento de informação ausente de seu ponto de vista (CHIO; FREEMAN, 2018).

A privacidade em sistemas de aprendizado de máquina deve ser um requisito importante, pois violações de privacidade geralmente têm consequências sérias e dispendiosas. Os sistemas de produção devem ser capazes de fornecer garantias de privacidade que sejam baseadas em estruturas teóricas e técnicas sólidas e limitem os

danos que os atacantes podem fazer para roubar informações privadas (CHIO, FREEMAN, 2018).

Big Data

Apesar de ser um termo muito utilizado na atualidade, o *Big Data* não possui nada de realmente novo, existem estudos sobre ele desde meados do século XX. O que difere o antigo *Big Data* do atual é a era digital. Com a evolução da sociedade, ferramentas mais efetivas foram inventadas, essas conseguem armazenar um maior número de dados e manipulá-los facilmente (MATRIZES; SCHROEDER, 2018).

A origem desses dados vem dos mais diversos locais: web, redes sociais, dados de transações, dados de biometria, dados gerados por pessoas e dados de máquina para máquina (*machine to machine*). Com isso surgiram termos para tentar explicar o objetivo de manter as plataformas e sistemas de *Big Data* em harmonia, sendo o mais usado os cinco V's: (GALDINO, 2016).

- volume: quantidade de dados acumulados;
- variedade: meios de propagação e tipos de dados;
- velocidade: taxa de transmissão dos dados;
- veracidade: confiabilidade dos dados;
- valor: resultado obtido do uso das ferramentas de *Big Data.*

Assim, surgiram desafios para essas ferramentas, sendo o principal a manipulação de dados, isto é, extrair valores através de correlações e processamentos, compreendê-los e aplicá-los no meio. Esse sistema de tratamento é feito utilizando algoritmos inteligentes, também chamados de "rede neural", e podem servir para os mais diversos fins, dependendo do desejo do manipulador de dados (GALDINO, 2016).

Em meio ao número crescente de dados disponibilizados, máquinas e pessoas interessadas em obter vantagens dessas informações, é inevitável que o *Big Data* seja uma ferramenta cada dia mais usada e em constante avanço. Imprescindível para a "Era Digital" (GALDINO, 2016).

Materiais e Métodos

Para o desenvolvimento do estudo e análise das questões de segurança e privacidade na utilização dos dados dos usuários na internet foi feito um estudo de caso do Cadastro Positivo existente, desde o ano de 2011 (Lei 12414/2011). Em 2019, esse cadastro passou por grandes mudanças que permitem acesso a mais informações e a dados de praticamente todos os brasileiros, desde dados simples, como nome, CPF, telefone, endereço; até os mais complexos, como padrão de consumo e pagamento de contas, tipos de créditos e serviços continuados contratados.

Cadastro Positivo

O Cadastro Positivo consiste de um banco de dados que reúne uma série de informações sobre os consumidores, como pagamento de compromissos relacionados à contratação de crédito (empréstimos, financiamentos e crediários) e histórico de pagamentos de contas de serviços continuados (água, luz, gás e telefone). (SERASA CONSUMIDOR, 2019).

Constarão no histórico da pessoa física (CPF) dados como: o valor total financiado, a quantidade e valor das parcelas, o comportamento e pontualidade de pagamento do consumidor. Com base nesses dados, pontuações (*scores* de crédito) serão calculadas e ações como atrasos ou não pagamentos a afetarão diretamente. Consequentemente, contratação de financiamentos ou créditos possuirão taxas de juros maiores ou menores, dependendo do comportamento do pagador (SERASA CONSUMIDOR, 2019).

Por fim, como comércios, bancos, financeiras e prestadores de serviços em geral obterão acesso a *score* de crédito, é inevitável que utilizem esses dados precisos para definirem condições comerciais e preços mais ajustados a cada perfil (SERASA CONSUMIDOR, 2019).

No dia 9 de maio de 2019, a Câmara dos Deputados aprovou o texto-base do projeto que modifica a Lei 12414, de 9 de junho de 2011. Essa mudança implementa ao Cadastro Positivo a mesma regra já existente para o cadastro negativo, ou seja, as instituições financeiras poderão incluir informações sobre seus clientes sem precisarem de suas autorizações específicas.

Lei 12414/2011 e Decreto 7829/2012 e 9936/2019

A Lei 12414, de 9 de junho de 2011, diz respeito a disciplinar a formação e consulta de bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Ela foi modificada em abril de 2019 pela Lei Complementar nº 166 de 08/04/2019, a qual a partir do Artigo 2º, inciso III (BRASIL, 2019b): "Cadastrado: pessoa natural ou jurídica cujas informações tenham sido incluídas em banco de dados", fez com que qualquer pessoa (física ou jurídica) fosse incluída no banco de dados do Cadastro Positivo, sem necessidade de autorização prévia.

Em meio a tantas mudanças, a dúvida que perdura é o quão seguros estão os dados dos cadastrados e quem realmente poderá consultá-los. Com base nisso, existia o Decreto 7829, de 17 de outubro de 2012, que foi revogado pelo Decreto 9936, de 24 de julho de 2019, que regulamenta a Lei nº 12.414, de 9 de junho de 2011, disciplinando a formação e a consulta a esse banco de dados. Apesar de incluir um capítulo que informa os procedimentos na hipótese de vazamento de informações (Capítulo VIII), o Decreto 9936/2019 não é muito transparente em relação a quais mecanismos serão usados para proteger os dados dos consumidores, limitando-se ao Artigo 16 para descrevê-los (BRASIL, 2019a): "Art. 16. O envio das informações pelas fontes aos gestores de bancos de dados será realizado por mecanismos que preservem a integridade e o sigilo dos dados enviados.". Além disso, o Capítulo VIII não informa o tipo de punição que será dada aos gestores de banco de dados que permitirem o vazamento de informações, dando uma impressão de impunidade, como pode ser visto no disposto:

> CAPÍTULO VIII
> DOS PROCEDIMENTOS NA HIPÓTESE DE VAZAMENTO DE INFORMAÇÕES
> Art. 18. Na ocorrência de vazamento de informações de cadastrados ou de outro incidente de segurança que possa acarretar risco ou prejuízo relevante a cadastrados, o gestor de banco de dados comunicará o fato:
> I - à Autoridade Nacional de Proteção de Dados, na hipótese de ocorrência que envolva o fornecimento de dados de pessoas naturais;
> II - ao Banco Central do Brasil, na hipótese de ocorrência que envolva o fornecimento de dados prestados por instituições autorizadas a funcionar pelo Banco Central do Brasil; e
> III - à Secretaria Nacional do Consumidor do Ministério da Justiça e Segurança Pública, na hipótese de ocorrência que envolva o fornecimento de dados de consumidores.
> § 1º A comunicação de que trata o caput será feita no prazo de dois dias úteis, contado da data do conhecimento do incidente, e mencionará, no mínimo:
> I - a descrição da natureza dos dados pessoais afetados;
> II - as informações sobre os cadastrados envolvidos;

> III - a indicação das medidas de segurança utilizadas para a proteção dos dados, inclusive os procedimentos de encriptação;
> IV - os riscos relacionados ao incidente; e
> V - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
> § 2º No juízo de gravidade do incidente de que trata o caput, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis para terceiros não autorizados a acessá-los.
> § 3º Será obrigatória a pronta comunicação aos cadastrados afetados pelo incidente de segurança de que trata este artigo (BRASIL, 2019a).

Estudo de Caso: Definição

O estudo de caso é uma estratégia de pesquisa que coloca questões do tipo "como" e "por que" em evidência e deve ser adotado em situações que o pesquisador tenha pouco controle sobre os eventos em estudo e quando o foco desse estudo são fenômenos contemporâneos (YIN, 2001).

Para a definição do caso em estudo é preciso compreender as questões que desejam ser abordadas pelo trabalho, elas definem o objetivo principal da pesquisa. No que se refere à síntese bibliográfica, buscou-se definir o direito do homem à sua privacidade, existindo legislações a respeito desse assunto desde o ano de 1948 (Declaração Universal dos Direitos Humanos). Portanto, há mais de 70 anos, o ser humano compreende que deve haver respeito às suas informações e dados, sendo vedado ao seu desejo compartilhá-los com outros ou não.

A Revolução Digital trouxe grandes avanços para a sociedade, inúmeras atividades que demoravam dias, semanas, até anos, passaram a ser realizadas em questão de segundos, minutos, horas, é inegável que os benefícios e vantagens de um mundo conectado vão além do que pode ser descrito. Porém, ainda não se tem definido até que ponto as empresas coletam e armazenam dados extras sobre seus consumidores, ou seja, dados que permitem compreender o comportamento e o pensamento de seus consumidores.

Com isso, adotou-se o Cadastro Positivo como objeto de estudo. Instaurado em 2011 e, até o início de 2019, era uma banco de dados cuja inclusão de informações dos consumidores era determinada pelo próprio consumidor. Com a mudança feita em abril, a inclusão será de todos os consumidores, sendo papel do consumidor informar o seu desejo de exclusão do banco de dados. Dessa maneira, o Serasa Consumidor terá acesso

a informações extras do consumidor: seu histórico de contratação de crédito e o seu padrão de pagamentos de contas de serviços continuados.

Com base nesses fatos e informações, chegou-se a quatro perguntas principais para nortear o trabalho:

1. Como as mudanças na legislação do Cadastro Positivo, referente à preservação da privacidade e segurança de dados dos consumidores, trabalham em relação aos consumidores?
2. Como os órgãos de defesa dos direitos dos consumidores se comportam a respeito disso?
3. Os consumidores têm conhecimento sobre as alterações da Lei nº 12.414, de 9 de junho de 2011? Em caso negativo, por que não?
4. Como a modificação do Cadastro Positivo pode auxiliar os consumidores e quais suas vantagens?

Dados coletados

Para o estudo de caso em questão, foi necessário coletar dados de diferentes tipos de fontes possibilitando uma análise com base em diversos pontos de vista. Para isso, dividiu-se o trabalho em quatro frentes: a opinião dos consumidores, a evolução do poder legislativo, o posicionamento dos órgãos de defesa dos consumidores e quais vantagens são apontadas por aqueles que trabalham com o Cadastro Positivo.

Essa divisão foi feita com base na extensa pesquisa bibliográfica apresentada durante a síntese, durante essa etapa do trabalho observou-se consumidores desinformados sobre o uso de seus dados, um poder legislativo em processo de desenvolvimento de leis, decretos e normas, e, por fim, um grande mercado de trabalho em crescimento para os profissionais da área.

Portanto, estabeleceu-se como objetivo principal:

1. determinar como as legislações que dizem respeito à preservação da privacidade e da segurança de dados dos consumidores trabalham a favor dos consumidores;
2. consultar como o órgão de defesa dos direitos dos consumidores (PROCON) se posiciona à respeito da mudança da Lei nº 12.414, de 9 de junho de 2011;
3. verificar se os consumidores têm conhecimento sobre as mudanças da Lei nº 12.414, de 9 de junho de 2011;

4. abordar as possíveis vantagens da alteração no Cadastro Positivo e como ele opera.

Para cada um dos tópicos aplicou-se uma técnica diferente para coleta de dados, adotando-se aquela que melhor se adequasse para cada público. As principais técnicas adotadas foram: entrevistas, questionários, participação em apresentação e pesquisa bibliográfica.

A primeira atividade desenvolvida para obtenção de dados envolvia entrevistar uma pessoa que tivesse conhecimento na área e, preferencialmente, trabalhasse e possuísse experiência em direito digital. A partir do momento que foi definida essa pessoa: um advogado, elaboraram-se as questões para a entrevista. As questões feitas ao entrevistado encontram-se no Quadro 1, informa-se que as repostas para as perguntas feitas foram disponibilizadas pelo entrevistado por meio de e-mail, tendo sido transcritas em sua totalidade.

Destaca-se que, além da entrevista, houve possibilidade de participação em uma apresentação sobre a Lei Geral de Proteção de Dados (LGPD), realizada às 19:00 (dezenove horas) do dia 19/08/2019, nas imediações das Faculdades Integradas de Araraquara (Av. Brasil, 782 – Araraquara/SP), pelos advogados Felipe Maciel e Jair Donizete Amando.

A segunda atividade desenvolvida diz respeito aos profissionais da área, tendo em vista que o Cadastro Positivo é um grande banco de dados que armazena informações sobre todos os consumidores brasileiros. É indiscutível que a área de coleta, armazenamento e utilização de dados/informações, possui um grande atrativo para os profissionais da área, pois está em constante evolução e desenvolvimento.

Portanto, apurou-se que seria necessário entrevistar um profissional que trabalhasse nessa área, ou até diretamente com o Cadastro Positivo, para compreender os atrativos da área e as possíveis vantagens da adoção desses bancos para os consumidores. Quando encontrado esse profissional, iniciou-se o processo de criação das perguntas que foram realizadas durante a entrevista (Quadro 1) realizada por meio de e-mail com as respostas transcritas em sua totalidade.

As perguntas diziam respeito a quais conhecimentos são necessários para trabalhar com o Cadastro Positivo, se o profissional sabia do que se tratava o cadastro em si antes de ingressar nessa área, quais as vantagens da utilização desse cadastro para o consumidor e, por fim, se esse profissional se descadastraria dessa ferramenta.

A terceira atividade elaborada visava verificar se o consumidor tinha conhecimento da mudança da lei 12.414/2011, se ele se considerava uma pessoa informada e se já sentiu invasão de sua privacidade enquanto utilizava redes sociais. Posteriormente informar sobre a alteração da lei e questionar sobre como se sente à respeito das informações recebidas.

Para questionar os consumidores, foi elaborado um Formulário Google que ficou ativo durante 31 dias (19/08/2019 a 19/09/2019). Não era necessário se identificar para responder ao questionário (anônimo) e sua divulgação foi feita por meio de redes sociais, comunicação direta com o público e folhetos colados nos corredores das Faculdades Integradas de Araraquara. No Quadro 1 disponibilizou-se as perguntas feitas no formulário.

A quarta e última atividade desenvolvida foi a de enviar um e-mail perguntando a Fundação de Proteção e Defesa do Consumidor do Estado de São Paulo (PROCON/SP) sobre seu posicionamento em relação à alteração da legislação, qual o efeito e como os consumidores devem se comportar com as mudanças. No Quadro 1 são informadas as perguntas enviadas para o e-mail edu.consumo@procon.sp.gov.br.

Quadro 1 – Perguntas realizadas durante as entrevistas.

Perguntas feitas durante a entrevista com o advogado Felipe Maciel
1. Quais seus conhecimentos sobre o direito digital? 2. Como você descreveria o crescimento desse ramo do direito em relação ao BOOM dos meios e métodos de coleta de informações e dados das pessoas online? 3. Você conhece alguma legislação, decreto, jurisprudência, entre outros, que dizem respeito ao direito digital? Quais? 5. Quais seus conhecimentos sobre o Cadastro Positivo? 6. Você soube sobre as alterações da Lei 12414 realizadas em abril de 2019? 7. Você acredita que essas mudanças podem permitir a distinção entre consumidores? 8. Como você enxerga a evolução do direito digital do consumidor? 9. E o contraste entre a rapidez da criação e implantação de novas tecnologias de coleta e armazenamento de dados em relação às etapas da tramitação de novos projetos de Lei sobre privacidade e segurança de dados (da sua apresentação até a publicação), qual são os efeitos desse processo para o cidadão?
Perguntas feitas para profissional que trabalha com o Cadastro Positivo
1. Fale sobre a sua experiência profissional, com o que já trabalhou, quais seus conhecimentos específicos e o que fez você ser atraído para essa área? 2. Depois que começou a trabalhar com isso, teve de estudar/aprender mais profundamente sobre quais temas? Qual teve maior dificuldade? 3. Na sua visão o que é o Cadastro Positivo? 4. Você tinha conhecimento dele antes de começar a trabalhar com esse tema?

5. Você poderia informar se tiveram muitas pessoas que pediram exclusão do cadastro? 6. Quais as principais vantagens de continuar cadastrado? 7. Você pensou em se descadastrar? Sob quais circunstâncias você tomaria tal atitude?
Perguntas feitas para os consumidores
• Ano de nascimento, escolaridade e sexo • Você acompanha algum tipo de noticiário? (televisivos, jornais, revistas, internet, rádio, entre outros). Se sim, qual(is)? Com que frequência? • Você possui alguma rede social? (Facebook, Instagram, Twitter, WhatsApp, Snapchat, Tik Tok, entre outras). • Como é o seu uso das redes sociais? • Você já sentiu que sua privacidade foi invadida por alguma rede social? • Você já sentiu insegurança em compartilhar dados em alguma rede social? • Você sabe o que é o Cadastro Positivo? • Você tinha conhecimento dessa informação? • Agora que tem conhecimento, você pretende pedir a exclusão do seu nome do Cadastro Positivo? Se sim, informe o porquê.
Perguntas feitas para o PROCON/SP
• Quais as principais vantagens e desvantagens para o consumidor ao integrar o cadastro positivo? • Vocês recomendam algum tipo de comportamento do consumidor? Ou seja, para ele é melhor continuar no cadastro positivo ou pedir exclusão de seu nome? • Se o consumidor se sentir lesado com o uso do cadastro positivo diante da contratação de algum serviço, por exemplo um financiamento, empréstimo, crediário, entre outros, como ele deve agir? Qual será o comportamento do PROCON/SP? • Como o PROCON/SP está agindo para defender os consumidores que decidiram/decidirem sair do cadastro positivo? No sentido de evitar que ocorra algum tipo de descriminação com eles.

Fonte: Autora (2019).

Definido o processo de coleta de dados foi possível fazer uma análise sobre o Cadastro Positivo e a invasão de privacidade, para isso serão usadas, como principais fontes para discussão, as duas entrevistas, o questionário ao consumidor e a síntese bibliográfica.

Resultados, Análise e Discussão

Com base nas respostas obtidas através das entrevistas e do questionário foi possível responder a maior parte das questões levantadas durante o desenvolvimento do estudo de caso. É importante destacar que a interpretação realizada das questões em

análise diz respeito à opinião do autor do trabalho, não refletindo, necessariamente, a opinião daqueles que participaram das atividades desenvolvidas.

Mudanças na legislação

As alterações ocorridas na Lei nº 12.414 afetam diretamente a privacidade e a necessidade de maior proteção dos dados dos consumidores. Como pode ser observado, a modificação realizada em abril permitiu a disponibilização de um grande número de informações e dados da população brasileira para o sistema de Cadastro Positivo.

No entanto, é inegável que a alteração ocorrida em abril piorou, tanto a preservação da privacidade, quanto a segurança dos dados dos consumidores. Em relação à perda de privacidade, tem-se que, a partir do momento que é permitido utilizar informações para definir valores e taxas para empréstimos, financiamentos, créditos, e consultar a *score* para avaliar o risco relacionado a possíveis compras e futuros clientes, existiu uma perda de privacidade, em comparação ao que ocorria anteriormente.

A segurança dos dados dos consumidores também foi prejudicada no sentido de que a empresa terá acesso a dados e informações que anteriormente não tinha. Sendo assim, será necessária a criação de novos mecanismos de proteção e segurança, proteger e ter preocupações com aquilo que antes nem existia.

No caso da segurança de dados deve ser lembrada da Lei Geral de Proteção de Dados, ela estabelece os parâmetros de segurança e as possíveis punições que podem ser aplicadas ao Serasa (empresa responsável pelos dados), em caso de divulgação ou perda de dados do Cadastro Positivo. Para isso, a LGPD estipula as sanções administrativas que vão desde uma advertência, uma multa simples (limitada a R$50 milhões) ou até a eliminação de todos os dados obtidos pela empresa.

Para o estudo de caso analisado, já existe uma legislação sobre a proteção de dados aprovada, publicada e que pode ser aplicada. Contrastando com o que se observa na prática, em que a tramitação das leis perante o Poder Legislativo é lenta, enquanto a criação e implantação de novas tecnologias são rápidas.

Durante a entrevista com o advogado Felipe Maciel, ele destacou que a tramitação de leis perante o Poder Legislativo é lenta por conta da alta demanda e as prioridades que as casas legislativas podem ter. Também destacou a necessidade da adequação do Direito à tecnologia, para que as leis possam evoluir como o mercado evolui. Para tanto, é

necessário uma maior discussão de temas específicos, como direito autoral, consumidor, cuidados na utilização das redes sociais, responsabilidade das empresas de tecnologia.

O modelo utilizado atualmente faz com que os possíveis impactos da utilização dos dados do cidadão no âmbito digital possam ser devastadores. Quando houver maior agilidade, possivelmente haverá maior segurança para o cidadão. Felipe Maciel também ressaltou que uma lei deve ser bem elaborada para atender às necessidades de qualquer cidadão, pois, existindo brechas, a instabilidade jurídica pode acarretar sérios problemas.

O PROCON/SP se posicionou desfavoravelmente à Lei Complementar nº 166/2019, por entender que as modificações trazidas acentuam a vulnerabilidade do consumidor em relação às instituições financeiras, além de afrontar o seu direito à privacidade.

Já em relação a sua atuação frente às alterações, ele destacou o artigo 17, parágrafo segundo, da Lei Complementar 166/2019:

> [...] os órgãos de proteção e defesa do consumidor poderão aplicar medidas corretivas e estabelecer aos bancos de dados que descumprirem o previsto nesta Lei a obrigação de excluir do cadastro informações incorretas, no prazo de 10 (dez) dias, bem como de cancelar os cadastros de pessoas que solicitaram o cancelamento [...].

Destacando que pelo artigo 17 dessa mesma lei, caso exista a quebra do sigilo previsto pela Lei Complementar nº 105, de 10 de janeiro de 2001 (dispõe sobre o sigilo das operações de instituições financeiras), a instituição estará cometendo um crime e estará sujeita à seguinte pena: "pena de reclusão, de um a quatro anos, e multa, aplicando-se, no que couber, o Código Penal, sem prejuízo de outras sanções cabíveis".

Conhecimentos dos consumidores

O questionário destinado aos consumidores foi respondido 64 vezes (Apêndice IV). No que diz respeito ao ano de nascimento, o formulário foi respondido em sua maioria (71,9%) pelos nascidos entre 1980 e 2010, integrantes da chamada "Geração Y e Z", entretanto destaca-se que houve respostas daqueles que nasceram em outros anos como os integrantes da geração *Baby Boomer* (4,7%), 1940 a 1960, e X (23,4%), 1960 a 1980.

Apesar das diferentes gerações, em relação ao grau de escolaridade, 100% dos que responderam ao questionário possuíam, pelo menos, o Ensino Médio completo. Desses, 53,1% apresentavam o Ensino Superior completo, entre os quais 35,9% tinham pós-

graduação. Com isso, pode-se afirmar que o formulário foi respondido por pessoas com grau de escolaridade adequado para o compreenderem e responderem corretamente.

Dentre os consumidores analisados, 60,9% eram do sexo masculino; e 39,1%, feminino; e 96,9% dos questionados disseram que acompanhavam algum tipo de noticiário. As principais fontes de notícia eram: o *site* G1 Notícias com 60,9%, os *feeds* das redes sociais (48,4%), o *site* Uol Notícias (42,2%) e o programa televisivo Jornal Nacional (29,7%). Pediu-se para indicarem uma frequência em que acompanham as notícias, o que gerou uma nota média de 5,39 em 10, portanto pode-se dizer que os consumidores se consideram por dentro das últimas informações que ocorrem no Brasil e no mundo.

Quando perguntado se esses consumidores apresentavam algum tipo de rede social, 95,3% disseram que sim e 68,7% indicaram um tempo de uso diário que varia de 0 a 4 horas. Quando diz respeito à privacidade e segurança nas redes sociais, 59,4% responderam que já sentiram que sua privacidade foi invadida e 81,3% sentiram insegurança em compartilhar seus dados.

As perguntas específicas para o estudo de caso obtiveram as seguintes respostas, 68,8% dos consumidores disseram que não sabiam o que era Cadastro Positivo; 71,9% não tinham conhecimento das recentes mudanças na Lei 12414/2011; 78,1% dos consumidores disseram que não pedirão exclusão de seu nome do Cadastro Positivo. Mas dos 21,9% que disseram que gostariam (14 pessoas), 11 (17,2%) informaram que o motivo pelo qual gostariam de ser excluídos seria a privacidade perdida.

Analisando esses dados, pode-se chegar às informações que já eram esperadas. Primeiramente, devido aos seus meios de divulgação, o questionário foi respondido por pessoas com alto grau de escolaridade e que nasceram após os anos de 1980. Essa geração foi a primeira a ter o acesso facilitado à internet, foi precursora da interatividade dentro de seus dispositivos e grande entusiasta e usuária das redes sociais. Portanto, era natural que, em sua maioria, possuísse algum tipo e a utilizasse diariamente.

Também é natural, que essa geração se tornasse usuária diária e que obtivesse suas notícias por meio de *sites* e até seus próprios *feeds*. Entretanto, destaca-se que esses usuários sentem que, em algum momento, tiveram sua privacidade e segurança invadidas, tornando-os cientes dos "perigos" da internet moderna (Internet das Coisas). Quando indagados sobre seus conhecimentos a respeito do Cadastro Positivo, era esperado que não tivessem um grande conhecimento, pois é um banco de dados novo, com apenas 8 anos, e que sofreu grandes alterações somente em abril desse ano.

Depois de tomarem ciência que seus dados seriam utilizados dentro desse banco de dados e quais seriam os efeitos para suas compras futuras, a maior parte dos consumidores informou que não pretende retirar seus dados. É importante lembrar-se do pensamento: "caso você tenha ganhado algo de graça no mundo digital, significa que você é o produto".

Portanto, muitos consumidores têm conhecimento de que dados disponibilizados, tanto nas redes sociais, quanto na internet, seriam e são fontes de informações para diferentes ferramentas, algoritmos, programas, entre outros, e é natural que com o tempo, os usuários compreendam que os termos de segurança e política de privacidade são muito mais do que um texto longo seguido de uma caixinha escrito "eu aceito". Aceitar significa ter ciência da perda de privacidade.

O Cadastro Positivo, os consumidores e os profissionais

A entrevista com o profissional que atuasse nesse mercado apresentou informações interessantes e mostrou que, apesar de seus pontos negativos; como perda de segurança e de privacidade dos consumidores, o principal objetivo do Cadastro Positivo é o de facilitar e melhorar a vida do consumidor.

Por meio da entrevista, foi possível averiguar que existe um mercado aberto, em constante evolução e crescimento para a sociedade que está em busca de um primeiro emprego, ou até mesmo, com dúvidas em relação ao seu futuro. O entrevistado destacou a tecnologia do *Big Data,* que a cada dia é mais e mais utilizada nos mais diferentes ramos da tecnologia e, tendo em vista a disponibilidade de dados, continuará nesse meio por muito tempo.

Além disso, foi importante para verificar que, apesar do questionário com os consumidores apresentar um resultado o qual a grande maioria não tinha conhecimento das recentes mudanças na Lei 12414/2011, o mesmo não ocorreu na realidade. Quando perguntado sobre o pedido de exclusão do cadastro, o entrevistado afirmou que houve pessoas que pediram para sair, tomando conhecimento de sua "perda" de privacidade e não a aceitando.

Por fim, compreendeu-se que, apesar dessa "perda" de privacidade e segurança, continuar no Cadastro Positivo pode ser a melhor opção para o consumidor, tendo em vista a seguinte resposta: "Os dados do Cadastro Positivo vêm para mostrar, através de indicadores, que mesmo que você tenha um débito pendente, isso não necessariamente

indica que você é um mau pagador". Ou seja, um consumidor pode estar no cadastro negativo por causa de uma conta que deixou de pagar. Porém, na hora de fazer um empréstimo ou financiamento, o banco levará em conta todo o seu histórico de pagamento, ou seja, sua pontuação (*score*), uma má ação do consumidor não atingirá outras noventa e nove boas. Suas condições serão melhores com o Cadastro Positivo.

Considerações Finais

O estudo de caso sobre as questões de segurança e privacidade na utilização dos dados dos consumidores no Cadastro Positivo promoveu uma análise que abrangeu diversos aspectos. Esse trabalho buscou pesquisar, por meio de uma síntese bibliográfica, a definição de privacidade e segurança, quais as legislações existentes e vigentes sobre esse tema, como as grandes empresas utilizam e como pretendem aplicar os dados disponibilizados pelos seus usuários e, por fim, quais as tecnologias usadas atualmente, que transformaram o tratamento de dados em uma ferramenta indispensável para qualquer empresa que deseja crescer e ser bem sucedida.

Através dessa pesquisa, definiu-se então qual seria o objeto a ser estudado: "o Cadastro Positivo", sendo o caso dividido em quatro objetivos principais de análise: a legislação existente para o Cadastro Positivo, como os órgãos de defesa dos direitos dos consumidores se comportam a respeito disso, qual a opinião dos consumidores em relação a esse banco de dados e quais as vantagens e desvantagens dessa nova ferramenta tanto para os usuários, quanto para os profissionais que trabalham na área, através da aplicação de diferentes técnicas de coleta de dados e informações (entrevistas, questionários, palestras, conversas informais, entre outros), chegou-se as conclusões:

- As mudanças ocorridas em abril na Lei 12414/2011 pioraram tanto a preservação da privacidade, quanto a segurança dos dados dos consumidores;
- Os consumidores costumam consultar notícias por meio da internet e de suas redes sociais. Entretanto, esses usuários sentem que em algum momento tiveram sua privacidade e segurança invadidas, tornando-os cientes dos "perigos" da internet moderna;
- Os consumidores não tinham conhecimentos sobre o Cadastro Positivo e depois de tomarem ciência do uso dos seus dados, a maior parte informou que não pretendia retirá-los dessa plataforma;

- Existe grande mercado em constante crescimento para os profissionais que desejam atuar nessa área, principalmente para aqueles que possuem conhecimentos sobre o *Big Data*;

Por fim, tem-se a grande questão para o consumidor: continuar cadastrado ou se descadastrar? Essa questão deve ser analisada pelo consumidor, se ele possuir como prioridade manter sua privacidade e segurança, ele pode se descadastrar. Porém, é importante dizer que existirá uma série de efeitos sobre a sua vida, como taxas diferentes ou possíveis dificuldades em fazer empréstimos, financiamentos etc.

Agora, se o consumidor já tem ciência de que seus dados são usados e não considera esse fato de extrema importância, poderá continuar no Cadastro Positivo. Tendo em vista que todo o histórico de compras será avaliado, serão muito maiores os benefícios de continuar nessa plataforma.

Referências

BRASIL. Decreto nº 592, de 6 de Julho de 1992. Atos Internacionais. Pacto Internacional sobre Direitos Civis e Políticos. Promulgação. **Diário Oficial**, Brasília, DF, 7 jul. 1992. Seção 1, p. 8716.

BRASIL. Decreto nº 7.829, de 17 de Outubro de 2012. Regulamenta a Lei nº 12.414, de 9 de junho de 2011, que disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. **Diário Oficial da União**, Brasília, DF, 18 de out. de 2012. Seção 1, p. 3.

BRASIL. Decreto nº 9.936, de 24 de Julho de 2019. Regulamenta a Lei nº 12.414, de 9 de junho de 2011, que disciplina a formação e a consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. **Diário Oficial**, Brasília, DF, 25 de jul. de 2019, 2019a. Edição 142, seção 1, p.1.

BRASIL. Lei Complementar nº 166, de 08 de abril de 2019. Altera a Lei Complementar nº 105, de 10 de janeiro de 2001, e a Lei nº 12.414, de 9 de junho de 2011, para dispor sobre os cadastros positivos de crédito e regular a responsabilidade civil dos operadores. **Diário Oficial**, Brasília, DF, 9 abr. 2019, 2019b. Edição 68, seção 1, p. 1.

BRASIL. Lei nº 12.965, de 23 de Abril de 2014 (Marco Civil da Internet). Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial**, Brasília, DF, 24 abr. 2014. Edição 77, seção 1, p. 1.

BRASIL. Lei nº 13.709, de 14 de Agosto de 2018 (LGPD). Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Diário Oficial**, Brasília, DF, 15 ago. 2018. Edição 157, seção 1, p. 59.

BRASIL. Lei nº 12.414, de 9 de Junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. **Diário Oficial**, Brasília, DF, 10 jun. 2011. Edição 111, seção 1, p. 2.

CANALES, Katie. **Microsoft just surpassed Alphabet's market cap for the first time in 3 years and the race to become the first trillion dollar company is heating up**. Bussiness Insider, New York, 29 maio 2018. Disponível em: https://www.businessinsider.com/microsoft-tops-alphabet-google-market-cap-2018-5?r=UK. Acesso em: 22 maio 2019.

CHIO, Clarence; FREEMAN, David. **Machine Learning and Security:** Protecting Systems with Data and Algorithms. California: O'Reilly, 2018.

DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS. Assembleia Geral das Nações Unidas em Paris. 10 dez. 1948. Disponível em: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/por.pdf. Acesso em: 18 mar. 2019.

FERREIRA, Aurélio Buarque de Holanda**. Miniaurélio**: o minidicionário da língua portuguesa.7. ed. Curitiba: Ed. Positivo; 2008.

GALDINO, Natanael. Big Data: Ferramentas e Aplicabilidade. *In*: SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA, XIII., **Anais[...]**. Rio de Janeiro: Faculdades Dom Bosco, 2016. Disponível em: https://www.aedb.br/seget/arquivos/artigos16/472427.pdf. Acesso em: 30 set. 2019.

GOOGLE. Privacidade & Termos: política de Privacidade do Google. Versão de 22 de janeiro de 2019. Disponível em: https://policies.google.com/privacy?hl=pt-BR. Acesso em: 9 maio 2019.

HUREL, Louise Marie; LOBATO, Luisa Cruz. **Segurança e Privacidade para a Internet das Coisas**. Instituto Igarapé, Nota Estratégica 31, nov. 2018. Disponível em: https://igarape.org.br/wp-content/uploads/2018/11/Seguranc%CC%A7a-e-Privacidade-para-a-Internet-das-Coisas.pdf. Acesso em: 9 maio 2019.

LIMA, Mariana. Aos 10 anos e com 2 bilhões de usuários, sistema Android mira emergentes. **O Estado de São Paulo**, São Paulo, 4 mar. 2018. Disponível em: https://link.estadao.com.br/noticias/cultura-digital,aos-10-anos-e-com-2-bilhoes-de-usuarios-sistema-android-mira-emergentes,70002212394. Acesso em: 22 maio 2019.

LUNDEN, Ingrid. **Amazon's share of the US e-commerce market is now 49%, or 5% of all retail spend**. Tech Crunch, San Francisco, jul. 2018. Disponível em: https://techcrunch.com/2018/07/13/amazons-share-of-the-us-e-commerce-market-is-now-49-or-5-of-all-retail-spend/. Acesso em: 22 maio 2019.

MICROSOFT. **Política de Privacidade da Microsoft.** Atualização: Abril de 2019. Disponível em: https://privacy.microsoft.com/pt-br/privacystatement. Acesso em: 14 maio 2019.

MONTEIRO, Renato Leite. **Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?**. Instituto Igarapé, Artigo Estratégico 39, Dez. 2018. Disponível em: https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf. Acesso em: 2 abr. 2019.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS NO BRASIL (ONUBR). **Artigo 12: Direito à Privacidade**. 2018. Disponível em: https://nacoesunidas.org/artigo-12-direito-a-privacidade/. Acesso em: 18 mar. 2019.

RODRIGUES, Leo. **Número de usuários de internet cresce 10 milhões em um ano no Brasil**. Agência Brasil, Rio de Janeiro, 20 dez. 2018. Disponível em: http://agenciabrasil.ebc.com.br/economia/noticia/2018-12/numero-de-usuarios-de-internet-cresce-10-milhoes-em-um-ano-no-brasil. Acesso em: 2 abr. 2019.

SCHROEDER, Ralph. Big data: moldando o conhecimento, moldando a vida cotidiana. **MATRIZes**, v. 12, n. 2, p. 135-163, ago. 2018. Disponível em: http://www.revistas.usp.br/matrizes/article/view/149604. Acesso em: 30 set. 2019.

STOUT, Dustin W. **Social Media Statistics 2019: Top Networks By the Numbers**. Dustin Stout, California, 2019. Disponível em: https://dustinstout.com/social-media-statistics/. Acesso em: 22 maio 2019.

SERASA CONSUMIDOR. **Como funciona o Cadastro Positivo?** 2019. Disponível em: https://www.serasaconsumidor.com.br/cadastro-positivo/. Acesso em: 1 ago. 2019.

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estud. av.**, São Paulo, v. 30, n. 86, p. 269-285, abr. 2016. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40142016000100269&lng=en&nrm=iso. Acesso em: 2 abr. 2019.

YIN, Robert K. **Estudo de caso:** planejamento e métodos. 2. ed. Porto Alegre: Bookman, 2001.