

DADOS PESSOAIS E O SEU VALOR

PERSONAL DATA AND ITS VALUE

Michael Douglas de Jesus Silva

Aline Alves Batista Leite

Rosa Maria Diekn de Queiroz

RESUMO

O presente artigo tem como objetivo apresentar uma análise da utilização dos dados pessoais nas grandes corporações. As transformações constantes no meio corporativo e tecnológico induzem o desenvolvimento de novas tecnologias, que em sua maioria, utilizam dados pessoais que podem tanto se referir ao nome e idade do usuário, mas como também conseguem identificar a personalidade. Quando o tema abordado se trata de dados pessoais, o debate parte para uma escala mundial, permitindo-se a recordação do caso ocorrido em 2016 pela agência Cambridge Analytics que no período pode ter sido o maior influenciador no rumo que as eleições americanas seguiram. A dispersão dos dados pessoais ocorrido na época mostra como as informações e a maneira que são utilizadas podem afetar a sociedade em grande escala.

Palavras-chave: utilização; dados pessoais; empresas; escala mundial.

ABSTRACT

This article aims to present an analysis of the use of personal data in large corporations. The constant changes in the corporate and technological environment induce the development of new technologies that mostly use personal data, which can refer both to the name and age of the user, but also to identify the personality of the user. When it comes to personal data, the debate starts on a global scale, allowing for the recall of the case in 2016 by Cambridge Analytics, which in the period may have been the biggest influencer in the direction that the American elections followed. The dispersion of personal data at the time shows how information and the way it is used can affect society on a large scale.

Keywords: utilization; personal data; companies; world scale.

INTRODUÇÃO

Milhões de usuários compartilham diversas informações sobre si mesmos em rede sociais, formulários, compras, transações etc. Esses dados quando isolados não possuem muita importância para as grandes empresas, porém, quando agrupadas e analisados passam a ter maior relevância, permitindo alterar padrões comportamentais de cada indivíduo sobre determinadas situações.

Grandes empresas como, Facebook, Google trafegam bilhões de dados diariamente entre seus sistemas e os bancos de dados. Logo, é possível levantar questionamentos, como: *“O que ocorre com esses dados? Se forem transferidos, para onde vão?”*. Essas informações são armazenadas, vendidas, analisadas e utilizadas em diversas situações pois, o produto de maior valor são os dados pessoais de cada usuário, porém, não estão referentes os dados como, fotos, contas, senhas entre outros; mas sim como cada usuário reage a uma foto, aonde aplicam suas finanças, onde e o que gostam de comprar. Assim, empresas que compram esses dados podem perfilar e avaliar como se portar em frente a esse usuário, utilizando como principal fator de influência, propagandas, imagens, anúncios que possivelmente serão exibidos para que o usuário possa tomar uma decisão mais favorável ao objetivo final da corporação. Por exemplo: Campanha do presidente eleito dos EUA, aonde a Cambridge Analytica avaliava os eleitores por meio de formulários, através de imagens, notícias, vídeos entre outras informações que são apresentadas no feed do Facebook. Os algoritmos que foram utilizados criam padrões de comportamento; o uso da psicométrica utilizada nas pesquisas da Cambridge Analytica permite a melhor identificação dos usuários, tanto no psicológico quanto na capacidade de prever decisões com muita precisão. Assim, podiam observar quais eleitores ainda poderiam ser influenciados para votar no presidente dos Estados Unidos, Donald Trump, que no período ainda era candidato à presidência.

Esses dados coletados podem não apresentar tamanha importância, mas é necessário lembrar dos termos de confidencialidade que foram assinados todas as vezes em que se é criado uma conta em uma rede social ou realizado download em algum aplicativo. Os termos não detalham que as informações podem ser utilizadas por terceiros a partir da permissão que se é concedida no primeiro acesso, ou seja, os dados são compartilhados sem nenhum controle por parte dos usuários. O emprego de tecnologias inteligentes para fins comerciais e políticos levanta uma

discussão sobre ética no meio tecnológico que ainda não se é discutido na sociedade, onde a regulação e sanção de leis que proteja os usuários continuam em fases iniciais.

O caso Cambridge Analytica

Envolvida em um escândalo em março no ano 2016, uma investigação dos realizada nos veículos jornalísticos The Guardian e o jornal de maior popularidade nos Estados Unidos, o The New York Times, revelaram que a empresa Cambridge Analytica possuía cerca de 50 milhões de dados pessoais de norte-americanos, porém os dados utilizados foram obtidos de forma irregular.

A Cambridge Analytica utilizava um algoritmo que perfilava a personalidade dos usuários do Facebook, não foi necessário a utilização de malwares ou outros tipos de invasões, pelo contrário, a conquista dos dados foi realizada de forma simples, através de interações como curtidas e compartilhamentos baseados no teste de personalidade chamado Big Five. O teste consiste em analisar cinco traços de personalidade de cada indivíduo, como, abertura a experiências, responsabilidade, extroversão, agradabilidade e irritabilidade. Segundo o teste Big Five, com base nesses 5 traços distintos quando unidos, é possível realizar uma divisão entre as pessoas com diferentes tipos de personalidades. A estratégia da empresa de tecnologia Cambridge Analytica foi baseada centralmente no Facebook, diretamente ligados as propagandas de forma que pudessem estabelecer algum tipo de comunicação com a usuário. O diretor digital de Trump Brand Parscale em uma entrevista prestada ao jornal CBS, disse de forma direta: “O Twitter é como [Trump] conversou com o povo, o Facebook como ele venceu” (Parscale, 2017). Parscale relata na entrevista que a campanha realiza constantemente mudanças nas tonalidades, efeitos, letras, fundo e frases nos anúncios publicados no Facebook, a fim de aumentar o impacto da propaganda. De acordo com Parscale, foi solicitado que os funcionários do Facebook aprendessem o máximo sobre a campanha de Hillary Clinton que na época era concorrente à Donald Trump na eleição. Segundo a Cambridge Analytica o algoritmo era tão preciso que com apenas 300 curtidas ele era capaz de identificar a sua personalidade melhor que seu cônjuge, mas eles não apenas analisavam isso, além das curtidas, eles analisavam comentários, posts e históricos. Em 2016 a Cambridge Analytica foi contratada pela campanha presidencial do atual Presidente dos EUA, Donald Trump, e o CEO da empresa, Alexander Nix, afirmava com base no teste do Big Five que sabia indicar cada personalidade de cada provável eleitor americano e com isso milhares de publicações enviadas diretamente

pra cada tipo de personalidade perfilado pelo algoritmo utilizando ciência comportamental, Big Data e publicidade personalizada levando em conta sexo, idade, religião e raça, já que todos os aspectos afetam diferentemente cada pessoa analisada. A repercussão no caso do escândalo da Cambridge Analytica causou uma repercussão que o ocorrido foi relatado em grandes jornais, possui livros que bordam a história e um documentário disponível na netflix chamado Privacidade Hackeada no qual apresenta os bastidores do escândalo de Cambridge Analytica juntamente ao Facebook. Após todo o episódio ocorrido o Facebook passou a suspender empresas de análise de dados no qual obtivesse suspeita de partilha de informações de usuários.

LEIS DE PROTEÇÃO DE DADOS

Após o escândalo ocorrido nos Estados Unidos envolvendo duas grandes empresas, Cambridge Analytica e Facebook, o assunto passou a ser tratado com maior cuidado e preocupação, onde em uma sociedade que é movida pelo compartilhamento e uso da informação, casos como o de Cambridge Analytica pode ser facilmente ocasionado novamente. Em virtude da proteção, o Brasil realizou a criação de uma lei que visa assegurar maior segurança aos usuários da internet em todo território nacional. Conhecida como Marco Civil da Internet, a lei brasileira visa aplicar uma regulamentação de dados pessoais a todas as empresas que coletam algum tipo de informação em território nacional, garantindo anonimização dos dados, as empresas podem coletar apenas dados que são considerados necessários para a realizar a ação no qual necessita do dado, quem ceder a informação para realizar algum serviço terá o direito de acesso à informação quanto poderá saber a finalidade daquele dado e quem os analisa, apresentada na constituição no capítulo 2 dos direitos e garantias do usuário, artigo 7º da lei Marco Civil da Internet:

“[...] VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
a) justifiquem sua coleta;
b) não sejam vedadas pela legislação; e
c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet [...]” (1988, LEI Nº 12.965, DE 23 DE ABRIL DE 2014.)

A lei brasileira foi baseada em uma lei já existente na Europa, chamada GDPR (General Data Protection) no qual estabelece a proteção dos usuários mediante as empresas que conseguem obter os dados dos usuários na internet, oferecendo ao usuário maior controle e transparência a respeito das informações pessoais armazenadas nos bancos de dados das corporações. A lei europeia na teoria seria inserida somente na Europa, porém, muitas empresas de diversos países se interessaram na lei e passaram inseri-la nos termos de privacidade, empresas como, Microsoft, Facebook, Spotify, Apple e Whatsapp já enviaram e-mails informando a atualização nas novas políticas de privacidade a partir da nova lei. A GDPR não define um limite de importância nos dados, ou seja, desde os dados mais detalhados sobre um usuário de uma rede social até os cookies de um site na internet são de grande relevância na lei. O usuário possui o direito de permitir quais dados podem ou não serem compartilhados, de acordo com a justificativa informada para solicitar um determinado dado, como também pode solicitar que os próprios dados de usuário salvos em uma determinada empresa possam ser apagados. Caso a empresa negue realizar os requisitos da lei, elas correm o risco de pagar multas que de acordo com o ocorrido podem variar entre 02% a 04% de seu faturamento anual.

Mesmo o Marco Civil da Internet sendo uma lei baseada na GDPR, as mudanças nos termos de uso e privacidade em diferentes aplicativos e redes sociais já foi apresentada a usuários brasileiros, pois, as empresas escolheram utilizar as diretrizes da GDPR em todos os países.

Figura 01 – Mensagem informativa da mudança nas diretrizes de uso e privacidade do Spotify



No Spotify, queremos oferecer a melhor experiência possível para garantir que você desfrute do nosso serviço hoje, amanhã e no futuro. Também é nosso objetivo ser o mais aberto e transparente possível com os usuários sobre os dados pessoais que coletamos para fornecer esse serviço, como são usados e com quem são compartilhados.

Estamos entrando em contato com você hoje para informar que faremos algumas alterações em nossa Política de Privacidade, que entrará em vigor a partir do dia 25 de maio. Essas alterações refletirão requisitos de transparência mais estritos do Regulamento Geral de Proteção de Dados da UE (conhecido como "GDPR").

Sempre nos esforçamos para fornecer informações claras e simples sobre os dados pessoais que coletamos e usamos, e como os protegemos em nossa Política de Privacidade. Hoje estamos simplesmente anunciando melhorias na Política de Privacidade que esclarecem e fornecem informações adicionais sobre:

- seus direitos de privacidade e como exercê-los:

Fonte: <https://www.techtudo.com.br/noticias/2018/08/lei-de-protecao-de-dados-na-internet-e-aprovada-no-brasil-entenda.ghtml>

PRINCÍPIOS DA PROTEÇÃO DE DADOS

É fundamental reforçar a cautela em relação a segura no tratamento de dados pessoais, a fim de precaver os usuários de exposições negativas e prejuízos de grande impacto. Um dos principais riscos quando há quebras de sigilo, invasão ou vazamento de informações é quando os dados passam a se tornarem públicos, ou seja, após a exposição de grande demanda de informações confidenciais/pessoais podem comprometer parte ou totalmente as ações e a vida social de uma pessoa ou empresa, tornando-as vulneráveis. Embora exista leis brasileiras que visam o intuito de aumentar a credibilidade na segurança dos dados, mesmo que submersos em uma era totalmente centralizada na tecnologia, não há nenhuma regulamentação específica sobre o uso de sistemas que coletam e processam dados de forma que possa realmente prevenir e reparar possíveis violações. Em meados de 1970, a agência com nível de gabinete americana dos Estados Unidos, Secretary for health, education and welfare (HEW), realizou uma comissão no qual foi divulgado um estudo que conclui pela relação direta entre a privacidade e os tratamentos de dados pessoais, com o objetivo de estabelecer uma regra que poderia controlar as próprias informações:

“A privacidade pessoal de um indivíduo é afetada diretamente pelo tipo de divulgação e utilização que é feita das informações registradas a seu respeito. Um tal registro, contendo informações sobre um indivíduo identificável deve, portanto, ser administrado com procedimentos que permitam a este indivíduo ter o direito de participar na sua decisão sobre qual deve ser o conteúdo deste registro e qual a divulgação e utilização a ser feita das informações pessoais nele contida. Qualquer registro, divulgação e utilização das informações pessoais fora destes procedimentos não devem ser permitidas, por consistirem em uma prática desleal, a não ser que tal registro, utilização ou divulgação sejam autorizados por lei [...]”. (DONEDA, 2010, p. 205).

Ideais como o apresentado, requer uma garantia de proteção aos cidadãos, com esse objetivo foi realizado a criação da lei nº 13.709 de 14 de agosto de 2018 prevê normas que visam proteger os direitos fundamentais da liberdade e da privacidade no tratamento de dados. As normas fundamentais da lei são:

“Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

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

I - o respeito à privacidade;

II - a autodeterminação informativa;

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

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

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.” (1988, LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.)

De acordo com o gerente executivo de política industrial da Confederação Nacional da Indústria pós ser sancionada (CNI), João Emílio Gonçalves, relata que muitas empresas estão adotando novos modelos de coleta e tratamento de dados para que possam se adequar as novas exigências da lei. Empresas do ramo de logística passam a ter mecanismos que controlam frota, o que demanda tratamento desses tipos de registros. Na entrevista à Agência Repórter o executivo explica:

“Empresas estão olhando negócios em transformação pela possibilidade de passar a incorporar cada vez mais serviços que dependem muito da coleta e tratamento de dados. Principalmente nas empresas líderes a gente vê uma atuação para se adaptar à lei. As empresas de maior porte elas mais ou menos atendem, estão mais preparadas para lidar com questão de tecnologia da informação (TI) e segurança da informação. Já firmas menores vão ter que fazer novos investimentos em TI. Acho que é um processo de aprendizado” (Agência Brasil, 2019).

A efetivação de tais princípios é uma melhoria no que se refere à autonomia governamental no objetivo da proteção de dados e a sua consideração ao direito fundamental. Outros países já sofreram alterações nas leis com o objetivo também de assegurar melhor credibilidade e segurança aos seus cidadãos, países como Espanha, Portugal e a lei GDPR já sancionada no continente Europeu são exemplos.

CONCLUSÃO

O presente artigo teve como objetivo analisar, questionar e entender como é realizado a utilização dos dados pessoais no meio tecnológico e quão valiosos podem ser para as empresas que os possuem. Analisando como são importantes as informações coletadas dos usuários para as grandes empresas, questionando como são manuseadas e como podem tornar alvos de grande escândalo quando compartilhadas com terceiros, lembrando casos como a ocorrida em 2016 com a Cambridge Analytica. Não isentando a possibilidade de ocorrer casos semelhantes, tendo em vista a perspectiva apresentada e os argumentos estudados, é possível elevar a ideia de quão necessário é a implementação de leis como, a Lei europeia GDPR, a Lei 12.965, denominada como Marco Civil da Internet e a Lei 13.709 no qual assegura os direitos fundamentais na proteção no tratamento de dados. Pode-se aludir que mesmo com a necessidade da implementação de leis, tratando-se de uma rede globalizada que é a internet, proteger os dados de forma totalmente segura é algo que ainda torna-se impossível, porém, é de grande relevância a importância da dissertação do tema referente à proteção de dados pessoais, quando se entende-se a amplitude dos benefícios e consequências que o compartilhamento e tratamento dos dados podem causar, onde as informações mesmo que sigilosas permanecem alocados em uma sociedade onde não há meios de manter total privacidade de suas informações.

REFERÊNCIAS

DONEDA, Danilo Cesar Maganhoto. Proteção de dados pessoais e relações de Consumo. In: A proteção de dados pessoais nas relações de consumo: para além da informação creditícia. Caderno de Investigações Científicas. Organizador: Danilo Cesar Maganhoto Doneda. Brasília: SDE/DPDC, 2010, p. 37-57.

EUA. Records, computers and the rights of citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems, 1973. Disponível em: <<https://www.justice.gov/opcl/docs/rec-com-rights.pdf> > Acesso: 20/10/2019.

BECKETT, L. Trump digital director says Facebook helped win the White House. The Guardian International Edition, 09 de outubro de 2017. Disponível em: <<https://www.theguardian.com/technology/2017/oct/08/trump-digital-director-brad-parscale-facebook-advertising>> Acesso: 20/10/2019.

Publico.pt. Cambridge Analytica acedeu a dados de 87 milhões de utilizadores. Publico.pt. 4 de abril de 2018. Disponível em: <<https://www.publico.pt/2018/04/04/tecnologia/noticia/cambridge-analytica-acedeu-a-dados-de-87-milhoes-de-utilizadores-1809156>> Acesso: 20/10/2019,

Marcelo Guerra Martins, Victor Augusto Tateoki. Proteção de dados pessoais e democracia: fake news, manipulação do eleitor e o caso da Cambridge Analytica. [s.d] Disponível em: <<https://revistas.unilasalle.edu.br/index.php/redes/article/view/5610>> Acesso: 21/10/2019

Janice Aparecida de Souza. Termos de Uso e Política de Privacidade. PUC Minas. 11 de setembro de 2019. Disponível em: <<http://periodicos.pucminas.br/index.php/virtuajus/article/view/21252>> Acesso: 21/10/2019.

Brasília. Brasília, 23 de abril de 2014; 193º da Independência e 126º da República. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.html > Acesso: 21/10/2019.

Brasília. Brasília, 14 de agosto de 2018; 193º da Independência e 126º da República. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso: 21/10/2019.

Emerson Alecrim. A controvérsia dos 50 milhões de perfis do Facebook manipulados pela Cambridge Analytica. [s.d]. Disponível em: <<https://tecnoblog.net/236612/facebook-cambridge-analytica-dados/>> Acesso: 21/10/2019.

Beatriz Cardoso. Lei de Proteção de dados na internet é aprovada no Brasil. 14 de agosto de 2018. Disponível em: <<https://www.techtudo.com.br/noticias/2018/08/lei->

de-protecao-de-dados-na-internet-e-aprovada-no-brasil-entenda.ghtml> Acesso: 21/10/2019.

Jonas Valente. Lei de proteção de dados traz desafios a empresas, cidadãos e governo. Agência Brasil. Publicado em 25 de agosto de 2019. Disponível em: <<http://agenciabrasil.ebc.com.br/geral/noticia/2019-08/lei-de-protecao-de-dados-traz-desafios-empresas-cidadaos-e-governo>> Acesso: 21/10/2019.