ISSN 2447-1097

Direito & TI – Porto Alegre / RS www.direitoeti.com.br

CORONAVÍRUS, ISOLAMENTO SOCIAL E A PRIVACIDADE DIFERENCIAL

Vytautas Fabiano Silva Zumas[1]

Dê-me sua alma, com metadados: Aceito! E assim se inicia uma relação em tempos digitais. Seria esse o novo modelo de "contrato social", ou melhor dizendo, comercial?

A cada dia mais e mais pessoas "assinam" os termos acima sem preocuparem-se com o seu preço. A busca por aplicativos e serviços, muitas vezes gratuitos, faz com que os usuários deixem de se preocupar com o que estão de fato fornecendo em troca, a sua privacidade.

Pode parecer simplório e sem muito valor agregado, mas os dados concedidos nesse pacto digital equivalem a verdadeira moeda corrente no ambiente cibernético. Empresas criam aplicativos e disponibilizam serviços gratuitos como forma de retribuir os dados fornecidos e coletados dos usuários que aceitam os termos e condições, na maioria das vezes sem sequer ler a política de privacidade da empresa.

Como exemplo analisado por Barreto e Santos (2020), o aplicativo russo *FaceApp* viralizou e foi baixado por milhões de pessoas no mundo todo. O que ele faz? Utiliza tecnologia de rede neural para literalmente (e de maneira bem convincente) alterar fotografias armazenadas ou tiradas com o próprio aplicativo para "envelhecer" os modelos fotografados.

Em troca da "brincadeira", a empresa russa coletou (e coleta) dos milhões de usuários dados como as próprias fotografias, dados fornecidos pelo usuário (a exemplo do endereço de e-mail), dados enviados pelo dispositivo (que podem conter a sua localização), informações de acesso a sites e aplicativos, registros de conexão e muito mais.

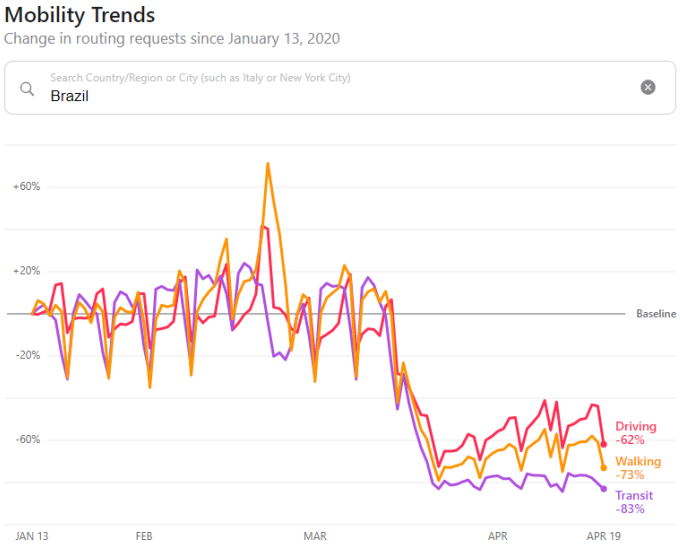
[1] Delegado de Polícia Civil do Estado de Goiás, tendo coordenado por dez anos o Grupo Especial de Repressão a Narcóticos e Grupo de Investigação de Homicídios da 11ª Delegacia Regional de Formosa. Exerceu suas atividades no Laboratório de Operações Cibernéticas do Ministério da Justiça e Segurança Pública e atualmente encontra-se mobilizado à Coordenação de Combate ao Crime Organizado da Diretoria de Operações no âmbito da Secretaria de Operações Integradas, também do MJSP. É professor e conteudista da Escola Superior da Polícia Civil do Estado de Goiás nas disciplinas Planejamento Operacional, Investigação de Homicídios, Investigação em Local de Crime, Interceptações Telefônicas e palestrante do tema Investigação e Telemática, de inimigas a grandes confidentes. É conteudista da disciplina de "INTELIGÊNCIA CIBERNÉTICA" do Curso de Aperfeiçoamento de Inteligência De Segurança Pública – CAISP, participou do Cyber Crime Investigation Course pela Gujarat Forensic Sciences University na cidade de Ghandinagar, Gujarat, Índia. Pertence ao corpo docente do Curso de Inteligência Cibernética da Diretoria de Inteligência da Secretaria de Operações Integradas do Ministério da Justiça e Segurança Pública. E-mail. vytautas.zumas@yandex.com.

Caso analisássemos a fundo a política de privacidade dos serviços oferecidos, veríamos que a gratuidade ofertada não seria tão justa assim. O *Face App* é apenas um exemplo da desigualdade no já citado "contrato comercial digital", assinado na maioria das vezes sem qualquer cautela.

Não estamos dizendo que tais serviços não devam ser utilizados ou que sejam prejudiciais, afinal de contas, só aceita quem quer. Os termos e condições estão lá desde o início e sempre à disposição. E mais, grandes empresas como Google, Apple e Facebook, em que pese a massiva coleta e armazenamento (consentidos) de nossa privacidade, oferecem produtos e serviços sem os quais já não vislumbramos a vida moderna.

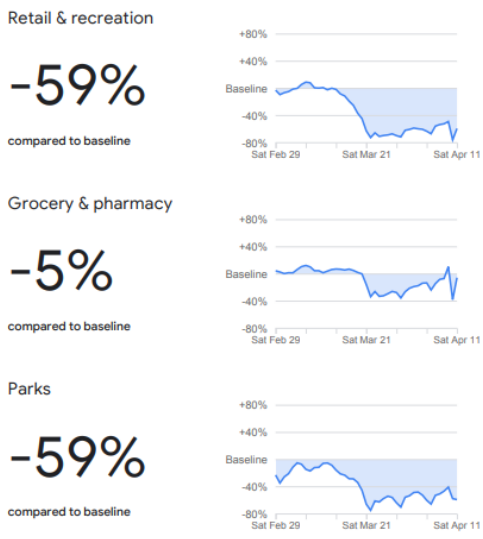
Mas o que chamou a atenção foi a recente disponibilização por parte das gigantes Google e Apple dos chamados Relatórios de Mobilidade Comunitária (*Community Mobility Report*[i]) ou Relatórios de Tendência de Mobilidade (*Mobility Trends Reports*[ii]), que nada mais são do que a divulgação da concentração de dispositivos (leia-se pessoas) em locais onde, teoricamente em razão da pandemia causada pelo Coronavírus, não deveriam estar.

Imagem 01: Mobility Trends Reports



Fonte: Apple (2020)

Imagem 02: Community Mobility Report



Fonte: Google (2020)

Na verdade, o que mais soou alarde não foi exatamente a ampla divulgação de tais dados, mas sim a reação dos usuários (diga-se de passagem, que "assinaram" o tal acordo), indignados e exigindo sua privacidade de volta.

Ora, desde o início, usuários Google e Apple concederam tal permissão e literalmente entregaram seus dados em troca dos produtos e serviços. O que ocorre é que a esmagadora maioria

deles sequer leu a política de privacidade antes de aceitar os termos. Não é agora que a destinação dos dados coletados não tem fins comerciais que os usuários deveriam se alarmar.

Ambas empresas afirmam que os dados publicados não são capazes de individualizar os usuários e tampouco feririam seus protocolos de preservação da privacidade.

É a chamada Privacidade Diferencial (*Differencial Privacy*) que, segundo a Google (2020), basicamente consiste na adição de "ruído" artificial aos seus conjuntos de dados, permitindo gerar *insights* e impedir a identificação de qualquer pessoa.

A privacidade diferenciada, aqui compreendida como teoria (gênero), consiste em técnicas de *machine learning* que, segundo tais empresas, oferecem fortes garantias matemáticas de que os modelos (máquinas) não aprendem ou se lembram dos detalhes sobre qualquer usuário específico[iii]. Especialmente para aprendizado profundo, as garantias adicionais podem fortalecer de maneira útil as proteções oferecidas por outras técnicas de privacidade, como o *TensorFlow Federated* (TFF), que consiste em uma estrutura de código aberto para aprendizado de máquina e outros cálculos em dados descentralizados[iv].

Sem embargo, e salvando o tema para discussão futura, suscitamos aqui a possibilidade da não inclusão "proposital" de ruídos artificiais aos conjuntos de dados das empresas coletoras de informações no contexto da Privacidade Diferencial. Assim, teoricamente e sem delongas técnicas, a *contrario senso*, tais empresas possuem o conhecimento de qual usuários está em determinado local em determinada data e horário.

Logo após a divulgação dos citados Relatórios de Mobilidade, o Governo do Estado de São Paulo divulgou, em 09/04/2020, que havia feito um acordo com as principais operadoras de telefonia móvel do país e iria "monitorar", através de mapas de calor, as maiores concentrações de dispositivos (leia-se pessoas) nas cidades do Estado.

A ação foi questionada pelo Ministério Público Federal através de ofício em caminhado no dia 12/04/2020 ao Governador do Estado e, em suma, teria o objetivo de "analisar se há potencial violação de direitos fundamentais da pessoa humana na execução do referido acordo, considerando que ele pode dar ensejo a mitigação do direito de intimidade e do direito de reunião – que, como sabido, não está ao alcance do poder normativo dos governos estaduais".

Apenas com efeito *inter partes*, um advogado obteve em sede de liminar em mandado de segurança decisão no sentido de que Governo de São Paulo exclua seu número de celular do sistema de monitoramento[v].

O sistema de monitoramento, divulgado pelo estado de São Paulo, nada mais é do que mais um acordo digital assinado sem a devida leitura pelos usuários. Afinal de contas, quem não precisa de um telefone celular nos dias de hoje? Para corroborar com a tese do contrato não lido, citamos, a

exemplo, as políticas de privacidade das empresas Vivo[vi] e Claro[vii] no tocante ao compartilhamento dos dados dos usuários.

A celeuma parece atual e inesperada, sendo a pandemia do Coronavírus talvez a motivação do alarde. Mas fato é que as grandes empresas provedoras de conteúdo, assim como de telefonia celular, já coletam e armazenam nossos dados há muitos anos e apenas agora a maioria das pessoas viram as bandeiras vermelhas.

A Google (2020) armazena, desde 2009, dados de localização de dispositivos no denominado *Sensorvault*, que se trata de um banco de dados interno da empresa contendo registros dos dados históricos de localização geográfica dos usuários desde a citada data. Assim, verificamos que a preocupação com nossos dados pode ter emergido um pouco tarde demais. Afinal de contas, como viveríamos hoje sem os sistemas operacionais Android (Google) e IOS (Apple)?

CONSIDERAÇÕES FINAIS

Eventos catastróficos, como a pandemia causada pelo Coronavírus, assim como a necessidade de isolamento social e consequentes medidas de empresas privadas e órgãos governamentais podem ter sido o "gatilho" para a conscientização dos usuários quanto a importância da manutenção da integridade de seus dados pessoais, assim como a importância da análise das políticas de privacidade de produtos e serviços muitas vezes disponibilizados a título gratuito na internet.

Ao não falar sobre a utilização de tais serviços por crianças, jovens e adolescentes, assim como a constante permissão de acesso integral à agenda de contatos, microfone e câmera de dispositivos, fazendo com a preocupação dos usuários mais atentos vá além do fato de que a Google ou Apple saibam que fomos às compras.

Frente à tais preocupações é fundamental e importante a consolidação de uma proteção de dados no Brasil, já consubstanciada na Lei Geral de Proteção de Dados, ainda em aguardo de início de vigência, pois que limita o poder de individuação dos dados pessoais e a identificação individual, circunstância não necessariamente vista como um direito legal, mas humano, pois que respeita o fundamental: a vida digna.

REFERÊNCIAS

APPLE. **Mobility Trends Reports**. Disponível em: https://www.apple.com/covid19/mobility. Acesso em: 21 abr. 2020.

BARRETO, Alesandro Gonçalves. DOS SANTOS, Hericson. FaceApp: será apenas este aplicativo a coletar nossos dados? **Revista Eletrônica Direito & TI**. 09 Mar. 2020. Disponível em http://direitoeti.com.br/artigos/faceapp-sera-apenas-este-aplicativo-a-coletar-nossos-dados/. Acesso em: 21 abr. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 24 nov. 2020.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm. Acesso em: 24 abr. 2020.

BRASIL. Tribunal de Justiça do Estado de São Paulo. **Decisão que autorizou parcialmente a liminar para afastar do minitoramento o "chip" do impetrante**. Mandado de Segurança nº 2.069.736-76.2020.8.26.0000 – São Paulo. Impte. CAIO JUNQUEIRA ZACHARIAS e Impdo. GOVERNADOR DO ESTADO DE SÃO PAULO. Relator Evaristo dos Santos e, 16 de abril de 2020 Disponível em: https://www.conjur.com.br/dl/liminar-exclusao-celular-monitoramento.pdf. Acesso em: 21 abr. 2020.

CLARO. **Política de Privacidade**. Disponível em: https://www.claro.com.br/politica-de-privacidade Acesso em: 21 abr. 2020.

GOOGLE. **Community Mobility Reports**. Disponível em: https://www.google.com/covid19/mobility/. Acesso em: 21 abr. 2020.

VIVO. **Política de Privacidade**. Disponível em: https://www.vivo.com.br/a-vivo/informacoes-aos-clientes/centro-de-privacidade/informacoes-coletadas/compartilhamento-de-dados. Acesso em: 21 abr. 2020.

TENSORFLOW. **TensorFlow Federated: Machine Learning on Decentralized Data**. Disponível em: https://www.tensorflow.org/federated. Acesso em: 21. abr 2020.

TENSORFLOW. **Introducing TensorFlow Privacy: Learning with Differential Privacy for Training Data.** Dosponível em: https://medium.com/tensorflow/introducing-tensorflow-privacy-learning-with-differential-privacy-for-training-data-b143c5e801b6. Acesso em: 21 abr. 2020.

[i] https://www.google.com/covid19/mobility/, acesso em 21 abr 2020.
[ii] https://www.apple.com/covid19/mobility, acesso em 21 abr 2020.
[iii] https://medium.com/tensorflow/introducing-tensorflow-privacy-learning-with-differential-privacy-for-training-data-b143c5e801b6, acesso em 21 abr 2020.
[iv] https://www.tensorflow.org/federated, acesso em 21 abr 2020.
[v] https://www.conjur.com.br/dl/liminar-exclusao-celular-monitoramento.pdf, acesso em 21 abr 2020.
[vi] https://www.vivo.com.br/a-vivo/informacoes-aos-clientes/centro-de-privacidade/informacoes-coletadas/compartilhamento-de-dados, acesso em 21 abr 2020.
[vii] https://www.claro.com.br/politica-de-privacidade, acesso em 21 abr 2020.