RECEBER DADOS ILEGALMENTE COLETADOS GERA RESPONSABILIDADE PELOS DANOS AOS TITULARES: o caso do compartilhamento de dados pelo aplicativo *Zoom* para o *Facebook*

Demócrito Reinaldo Filho
Desembargador do TJPE

Numa época em que as pessoas passaram a fazer quase todas as atividades em meio digital, um aplicativo de videoconferência tornou-se a plataforma social da era do coronavírus. Com escolas fechadas e milhões de pessoas trabalhando de casa, o *Zoom* se tornou enormemente popular. Trata-se de um aplicativo muito funcional, porque permite criar salas privadas e dezenas de pessoas se plugarem na sala virtual ao mesmo tempo. O recurso é útil para garantir que apenas convidados entrem na reunião *on line*, impedindo participação de usuários que não foram convidados. O aplicativo é fácil de usar e de rápida instalação.

As pessoas estão usando o *Zoom* não somente para ministrar conferências e aulas de cursos regulares, realizar encontros de negócios, sessões de terapia, consultas médicas, reuniões familiares, aulas de ginástica e de música, mas até para "festas virtuais" ele tem sido utilizado. O aplicativo tornou-se importante ferramenta para escolas, escritórios, comunidades e grupos de amigos, que o utilizam como instrumento para sociabilização ou simplesmente para atenuar as agruras do isolamento social.

O aplicativo foi lançado em 2011 como ferramenta de videoconferência para o setor de negócios. Contava com cerca de 10 milhões de usuários em todo o mundo

no final de dezembro de 2019, entre usuários gratuitos e os que assinam algum plano pago do serviço. Durante o mês de março deste ano, como resultado da pandemia da Covid-19, o *Zoom* tornou-se praticamente onipresente, pois se difundiu extensamente e deixou de ser aplicativo restrito ao mundo dos negócios. Desde 18 de março é o aplicativo mais baixado na *App Store* e na *Google Play*, tendo alcançado a marca de 200 milhões de usuários[1]. Nas últimas semanas, mais de 90 mil escolas em 20 países adotaram o *Zoom* como plataforma de ensino a distância.

O lado negativo do crescimento desmesurado logo se fez sentir. Defeitos de segurança apareceram na mesma proporção da disseminação do *Zoom*. Diversos *bugs* e falhas na arquitetura do aplicativo permitiram exploração das brechas por *hackers*, que tiveram acesso a dispositivos dos usuários[2]. As vulnerabilidades da ferramenta de videoconferência foram exploradas por invasores, que conseguiram acessar a câmera e o microfone de usuários e conteúdos das reuniões realizadas na plataforma. Uma nova forma de ataque virtual emergiu da crise de insegurança do *Zoom*, com direito a neologismo - "Zoombombing", a prática utilizada por *hackers* de entrar numa sala virtual, apoderar-se dos comandos e postar conteúdos ilícitos, como material racista, preconceituoso ou pornográfico, como forma de constranger e chocar os demais participantes[3].

---

[1] Ver reportagem publicada em 04.04.20 pela CNBC, acessível em: https://www.cnbc.com/2020/04/03/how-zoom-rose-to-the-top-during-the-coronavirus-pandemic.html

[2] Ver reportagem publicada em 01.04.20, sob o título "Zoom Bug Gives Hackers Full Control Over Computers", acessível em: https://www.inc.com/don-reisinger/zoom-bug-gives-hackers-full-control-over-computers.html

[3] Professores de Singapura deixaram de utilizar o *Zoom* para realizar vídeo aulas por causa de um incidente desse tipo. Durante uma aula de geografia, hackers invadiram a sala virtual e postaram comentários obscenos e conteúdo pornográfico. Ver reportagem publicada em 10.04.20 pela BBCNews, acessível em: https://www.bbc.com/news/world-asia-52240251

Diversos outros problemas e escândalos surgiram nas últimas semanas, e as pessoas começaram a se perguntar que tipo de dados o aplicativo coleta e o que faz com as informações dos usuários. Uma enxurrada de críticas emergiu, com acusações sobre medidas de segurança inadequadas, ausência de criptografia e uma política de privacidade que permitia compartilhamento com terceiros.

Milhares de vídeos gravados com a plataforma *Zoom* foram encontrados na *web*, expostos sem proteção. Os vídeos incluíam conteúdo íntimo e altamente sensível, como encontros de negócios, sessões de terapia e até mesmo cenas de nudez[4]. Uma análise do *The Intercept* revelou que as comunicações por vídeo na plataforma não são criptografadas de ponta a ponta, ao contrário do que seu site e seu *white paper* de segurança proclamavam. Em seguida, descobriu-se que o aplicativo enviava informações para o *Facebook*, sem que os usuários tivessem sido previamente alertados.

O fundador e CEO da empresa *Zoom Video Communications Inc.*, Erin Yuan, pediu desculpas públicas[5] e prometeu resolver os problemas[6]. Algumas medidas adicionais

---

[4] Os vídeos vazaram pela falta de cuidado no momento de armazenar os arquivos. As mídias foram armazenadas de forma desprotegida em um dos servidores da *Amazon Web Services*. Ver reportagem publicada pela *Forbes* no dia 04.04.20, sob o título "New Zoom User Blow: This Is How 'Thousands' Of Video Chats Are Available For Anyone To View Online", acessível em: https://www.forbes.com/sites/kateoflahertyuk/2020/04/04/new-zoom-user-blow-this-is-how-thousands-of-video-chats-are-available-for-anyone-to-view-online/#31d2aa62785d

[5] É o seguinte o trecho onde o fundador e executivo-chefe da *Zoom* pede desculpas (no original, em inglês): "However, we recognize that we have fallen short of the community's – and our own – privacy and security expectations. For that, I am deeply sorry, and I want to share what we are doing about it."

[6] O executivo divulgou uma mensagem aos usuários, no dia 1°. de abril, onde alinhavou as medidas que a empresa já tinha tomado para consertar os defeitos de segurança do aplicativo. Ver o teor da mensagem em: https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/

de segurança já foram adotadas[7], e a empresa está trabalhando na implantação de um sistema de criptografia.

Isso, contudo, não foi suficiente para estancar os prejuízos à imagem da empresa e do seu produto, iniciando-se um processo de reversão da popularidade do aplicativo. Diversas empresas e órgãos públicos, em várias cidades e países, proibiram a utilização do *Zoom*. A *Google*, ciente das falhas de segurança do aplicativo, impediu seus empregados de instalar o aplicativo em seus equipamentos. A SpaceX e a *Tesla*, companhias do bilionário Elon Musk, o Departamento de Educação da cidade de Nova York e Taiwan também bloquearam a instalação da plataforma, temendo que seus funcionários tivessem reuniões espionadas[8].

A empresa ainda enfrenta problemas de outra ordem, submetida a procedimentos investigativos.

A Procuradora Geral do Estado de Nova York (EUA), Letitia James, abriu investigação para escrutinar as políticas de segurança e privacidade adotadas pela *Zoom Video Communications Inc.* em relação ao aplicativo. Numa carta enviada no dia 30 de março, requereu informações sobre como estão sendo implementadas as novas medidas de

---

[7] A exemplo da criação de uma "waiting room", um estágio que qualquer interessado em ingressar num determinado grupo tem que passar antes de ter acesso à "sala do encontro" (*meeting room*). O anfitrião (*host*) do encontro, então, tem tempo para permitir a entrada no grupo (*meeting room*) entre aqueles que estão na sala de espera (*waiting room*) - ver reportagem publicada em 03.04.20, sob o título "Zoom ads new security and privacy measures to prevent Zoombombing", acessível em: https://www.theverge.com/2020/4/3/21207643/zoom-security-privacy-zoombombing-passwords-waiting-rooms-default. Além disso, foi instituído um sistema de senha adicional (*two-factor authentication*), necessária para se ingressar em uma sala virtual. Antes, somente era necessário a senha inicial, para ingressar no próprio aplicativo. Agora é preciso que o usuário tenha uma segunda senha, adequada para o grupo que se quer ingressar - ver reportagem publicada em 05.04.20, sob o título "Zoom Meetings Just Got Safer", acessível em: https://www.inc.com/don-reisinger/zoom-bug-gives-hackers-full-control-over-computers.html

[8] Ver reportagem publicada em 08.04.20, no site *Olhar Digital*, acessível em https://olhardigital.com.br/coronavirus/noticia/google-proibe-funcionarios-de-utilizarem-o-aplicativo-zoom/99237.

segurança, para lidar com o enorme aumento de uso do aplicativo e proteger contra invasões de hackers[9].

No Brasil, a Agência Nacional de Vigilância Sanitária (Anvisa), órgão vinculado ao Ministério da Saúde, proibiu a instalação do aplicativo nos computadores internos da agência[10]. No dia 08 deste mês, o Ministério da Justiça e Segurança Pública, por meio do Departamento de Proteção e Defesa do Consumidor (DPDC), da Secretaria Nacional do Consumidor (SENACON), abriu investigação formal contra a empresa controladora do aplicativo *Zoom*. O DPDC quer esclarecer pontos sobre o compartilhamento de dados com o Facebook e notificou a empresa para prestar esclarecimentos[11].

Um dos aspectos que mais influenciou a abertura de procedimentos investigados contra a empresa que desenvolve o *Zoom* foi a revelação de que o aplicativo repassava informações dos seus usuários ao *Facebook*. Não somente porque esse ponto revelou conduta antiética da empresa, mas em razão de que a simples menção de o *Facebook* estar envolvido no problema é suficiente para despertar elevados temores quanto à privacidade dos usuários. O Facebook esteve no centro de alguns dos maiores escândalos de invasão de privacidade e uso indevido de dados pessoais nos últimos tempos. Não custa lembrar o caso da *Cambridge Analytica*, empresa que recebia dados compartilhados pelo

---

[9] Ver reportagem publicada pelo *New York Times* em 30.03.20, acessível em: https://www.nytimes.com/2020/03/30/technology/new-york-attorney-general-zoom-privacy.html

[10] Ver reportagem publicada no site da *UOL*, em 06.04.20, acessível em: https://noticias.uol.com.br/ultimas-noticias/agencia-brasil/2020/04/06/anvisa-proibe-uso-interno-do-app-zoom-por-problemas-de-seguranca.htm

[11] A empresa tem o prazo de 10 dias para prestar os esclarecimentos solicitados. Caso a empresa controladora do *Zoom* não responda no prazo estipulado ou haja mais indícios de violação de direitos dos consumidores, o MJSP poderá instaurar processo administrativo, que eventualmente poderá resultar na imposição de multa. Ver, a esse respeito, notícia publicada no site Convergência Digital, no dia 08.04.20, acessível em: http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=53325&sid=4

Facebook e os utilizava para outras finalidades, sobretudo para influenciar resultados de eleições em diversos países.

Antes de definir a responsabilidade da empresa responsável pelo *Zoom* e também do Facebook, pelo compartilhamento indevido dos dados dos usuários, é preciso entender um pouco melhor como funciona o aplicativo e como questões relacionadas à privacidade se encontram tão envolvidas com o seu funcionamento.

A preocupação com a privacidade dos usuários em relação a aplicativo como o *Zoom*, que permite videoconferências, é inata ao seu funcionamento. Todas as conversas podem ser gravadas, mensagens transcritas, arquivos enviados são copiados, documentos armazenados e tudo o que as pessoas distribuem durante os encontros virtuais pode ser visto e replicado. Além disso, os nomes das pessoas que participam dos encontros ficam registrados. O "anfitrião do encontro" (*meeting host*) também obtém informações e pode compartilhá-las. Não é apenas a empresa que desenvolve o *Zoom* que coleta informações pessoais dos usuários. A arquitetura do aplicativo permite que o anfitrião (*host*) do encontro – o usuário que faz o cadastro e agenda a reunião virtual – também fique em poder de um grande volume de dados. Ele pode gravar a conferência, transcrevê-la automaticamente e compartilhar os vídeos e informações com pessoas que não estejam na sala do encontro virtual (*meeting room*)[12]. Quando o encontro é gravado, o anfitrião tem a opção de armazenar o material no seu próprio dispositivo (terminal de acesso) ou na nuvem (*cloud*) da empresa.

Como se percebe, a preocupação com a privacidade dos utentes de um aplicativo de

[12] Embora, a partir de mudanças implementadas na arquitetura do aplicativo, agora os participantes são notificados quando o anfitrião (*meeting host*) está gravando o evento e têm a opção de ficar ou deixar o encontro.

videoconferência é extrema, devido à grande variedade e volume de informações coletadas e que, se utilizadas inadequadamente, podem causar estragos enormes à esfera dos direitos da personalidade dos indivíduos.

No caso do compartilhamento de dados com o *Facebook*, o problema estava na falta de informação sobre esse aspecto do funcionamento do aplicativo. A empresa controladora da plataforma *Zoom* não informava aos usuários que partilhava seus dados com a rede social nem qual uso esta última poderia fazer com os dados repassados.

A prática foi descoberta após o site *Motherboard* publicar análise da versão do aplicativo para o sistema operacional *iOS*[13]. De acordo com a publicação, após o usuário fazer o *download* e instalar o *app*, ele se conecta à *SDK* do Facebook, que vem a ser a porta de entrada e saída de dados da rede social. O *SDK* (*Software Development Kit*)[14] é uma das ferramentas de negócios que a *Facebook Inc.*, empresa que controla a rede social, fornece a seus parceiros. As "ferramentas de negócios" são tecnologias que o Facebook oferece a proprietários e editores de sites, programadores de aplicativos e empresas com as quais tem algum tipo de parceria. Essas tecnologias facilitam a integração dos aplicativos e sites parceiros com o Facebook, permitindo troca de dados, compreensão do

---

[13] **iOS** é um sistema operacional móvel da Apple Inc. desenvolvido originalmente para o *iPhone*, mas também usado no *iPod touch* e *iPad*. A Apple não permite que o *iOS* seja executado em *hardware* de terceiros. As versões principais do *iOS* são lançadas anualmente.

[14] **Kit de desenvolvimento de software**, também conhecido como ***Software Development Kit***, ***SDK*** ou **"devkit"**, é um conjunto de ferramentas de desenvolvimento de software que permite a criação de aplicativos para uma plataforma, um sistema operacional de computador, um console de videogame etc. Para criar aplicativos para esses sistemas e plataformas, deve-se utilizar um kit de desenvolvimento de software específico, formando um ambiente de desenvolvimento integrado. Normalmente os SDKs são disponibilizados pelas empresas para que programadores externos tenham uma melhor integração com a plataforma (ou sistema) e para encorajar o uso dela (cf. Wikipedia).

funcionamento e medição da atividade dos produtos dos parceiros[15].

Após a prática ilícita ser descoberta, a companhia atualizou o aplicativo *Zoom*, removendo o *SDK* do Facebook[16], que o conectava à rede social[17]. Em nota publicada em 27 de março, a empresa explicou que implementou a configuração de "login com o Facebook" usando o Facebook *SDK* para *iOS* de modo a fornecer aos usuários um modo simples e conveniente de acesso à plataforma. Todavia, ao tomar conhecimento (naquele dia) de que o *SDK* coletava informações desnecessárias ao funcionamento do aplicativo, decidiu removê-lo no cliente *iOS*. Explicou ainda que, para essa mudança ter eficácia, é necessário que os usuários façam atualização do aplicativo para a versão mais nova[18]. A *Zoom Video Communications Inc.* afirmou que nenhuma informação pessoal era repassada, apenas dados sobre o aparelho, versão do sistema operacional, horário dos *logs*, operadora utilizada, modelo do dispositivo, tamanho da tela, poder de processamento e espaço de armazenamento[19].

Apesar de ter providenciado a desinstalação ou reconfiguração do *SDK*, essa providência não isenta a *Zoom Video Communications Inc.* pelos danos causados aos titulares dos dados indevidamente compartilhados. Da mesma

---

[15] O Facebook informa quais são as "ferramentas de negócios" que utiliza na integração com os produtos de seus parceiros. Ver em: https://www.facebook.com/help/331509497253087

[16] Ver notícia publicada em 03.04.20, pelo site *IG*, sob o título "Zoom é seguro? Entenda os escândalos de privacidade envolvendo o aplicativo", acessível em: https://tecnologia.ig.com.br/olhar-digital/2020-04-03/zoom-e-seguro-entenda-os-escandalos-de-privacidade-envolvendo-o-aplicativo.html

[17] Numa mensagem aos usuários publicada em 01.04.20, a empresa afirmou que havia feito a remoção do *SDK* do Facebook e reconfigurado de modo a prevenir que colete informação desnecessária sobre os dispositivos dos usuários. Ver inteiro teor da mensagem em: https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/

[18] Liberada na mesma data (27/3). Ver nota formal da empresa sobre a remoção do SDK do Facebook, publicada em 27.03.20, disponível em: https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/ https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/

[19] Ver notícia referenciada na nota anterior.

forma, a Facebook *Inc.* responde solidariamente, por ter feito uso de dados repassados sem autorização dos titulares.

Dois aspectos desfavorecem ambas as empresas. O primeiro reside na ausência de informação adequada aos usuários do aplicativo *Zoom*, que não tinham conhecimento de que seus dados eram repassados para o Facebook. O segundo diz respeito à questão da qualidade dos dados compartilhados, que não se resumiam a simples "metadados", como alegado.

A política de privacidade do aplicativo *Zoom* não informava que sua versão *iOS* enviava dados para o *Facebook*, mesmo daqueles usuários que não tinham conta na rede social. A política de privacidade do *Zoom* era muito ampla, quase sem limites, permitindo que coletasse dados dos usuários praticamente de forma ilimitada[20]. O *Zoom* coletava informações pessoais de seus usuários e não fornecia qualquer detalhe sobre como os dados eram usados para publicidade, marketing e outros propósitos comerciais. Vídeos, anotações e qualquer tipo de gravação de voz poderiam ser armazenados e até compartilhados com terceiros não integrantes dos encontros virtuais.

Somente após a publicação de um artigo na *Consumer Reports*[21], em 24 de março, é que a empresa decidiu fazer ajustes na sua política de privacidade[22]. Num anúncio publicado no dia 29 de março, a empresa confirmou que atualizou sua política de privacidade para dar mais transparência sobre que tipo de dados coleta e qual uso faz da informação coletada. Enfatizou que não vende os dados que recolhe nem monitora o conteúdo dos vídeos dos encontros realizados por meio de sua plataforma. Informou

---

[20] https://zoom.us/privacy

[21] A notícia foi originalmente publicada no dia 24.03.20 e está disponível em: https://www.consumerreports.org/video-conferencing-services/zoom-teleconferencing-privacy-concerns/

[22] https://zoom.us/privacy

que coleta basicamente informações técnicas, como endereço *IP* do usuário e detalhes do seu dispositivo. Informou ainda que, a não ser que o anfitrião (*host*) faça gravação dos arquivos de vídeo, áudio e das conversas (*chats*) trocadas durante um encontro (teleconferência), ela não armazena esse material[23]. Enfatizou que "nenhum dado relativo à atividade do usuário na plataforma *Zoom* – incluindo vídeo, áudio ou conteúdo de *chat* – é fornecido a terceiros para fins de publicidade"[24].

A alteração tardia da política de privacidade não faz desaparecer a responsabilidade da empresa. Para compartilhar dados, é indispensável que o controlador de um sistema informático obtenha consentimento do titular. A empresa que controla o *Zoom* tinha consentimento para coleta dos dados, necessários ao funcionamento do aplicativo. O consentimento fora obtido exclusivamente para essa finalidade. Se o processamento dos dados foi autorizado apenas para uma finalidade específica, não poderiam ser utilizados para objetivos diversos. Se a empresa obteve consentimento dos usuários para tratamento de seus dados pessoais em atividade determinada, não poderia utilizá-los para outros propósitos, muito menos compartilhá-los com terceiros para finalidades estranhas à informada ao titular dos dados no momento em que o consentimento fora solicitado. O operador ou controlador que necessitar comunicar ou compartilhar dados pessoais com terceiros deve obter consentimento específico do titular dos dados para esse fim, sob pena de ofensa ao princípio da finalidade. Esse princípio obriga a que qualquer atividade

---

[23] Ver a declaração em: https://blog.zoom.us/wordpress/2020/03/29/zoom-privacy-policy/

[24] "No data regarding user activity on the Zoom platform – including video, audio, and chat content – is ever provided to third parties for advertising purposes.".

de tratamento de dados tenha fim específico, previamente informado ao titular, sem possibilidade de tratamento posterior de forma diversa da finalidade anunciada. O controlador que consegue consentimento para utilizar dados pessoais com exclusividade, mas depois necessita comunicar ou compartilhar os dados com outros controladores, tem que obter novo consentimento específico do titular para esse fim.

O princípio da finalidade, um dos que caracterizam o tratamento de dados legítimo, foi incorporado ao nosso ordenamento jurídico pelo art. 7°., inc. VIII, alíneas *a* a c, da Lei n. 12.965/14 ("Marco Civil da Internet"). A Lei Geral de Proteção de Dados (LGPD - Lei n. 13.709/18) também consagra o princípio da finalidade como uma das condições para a licitude da atividade de tratamento de dados (art. 6°., I)[25]. Embora a LGPD só entre em vigor em agosto, seus preceitos já servem como baliza norteadora da legitimidade de qualquer atividade que implique utilização de dados pessoais.

O compartilhamento de dados pessoais sem conhecimento do titular ofende outras regras e princípios do sistema normativo, a começar pelo dever de informação que é atribuído a todo fornecedor, nas relações de consumo (arts. 4°, IV, e 6°., II e III, do CDC – Lei 8.078/90). O dever de informação se traduz num dever de aviso e esclarecimento, no sentido de que o sujeito que se encontra informado sobre um fato que tenha influência no consentimento da outra tem obrigação de prestar os devidos esclarecimentos. Compartilhamento de dados não consentido

---

[25] "Art. 6° As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;"

também constitui prática comercial abusiva (art. 39 do CDC), já que a omissão quanto à repartição dos dados é forma enganosa de atrair o consumidor - que quando tem conhecimento prévio do compartilhamento, geralmente não adquire o produto.

A jurisprudência brasileira é no sentido de que o compartilhamento de informações sem prévio conhecimento e autorização do consumidor (titular dos dados) gera o direito à indenização por **danos morais**. Esse entendimento ficou assentado em caso recente, julgado pela 3ª. Turma do Superior Tribunal de Justiça, que condenou um gestor de banco de dados a indenizar um consumidor pela comercialização indevida de informações pessoais. Para a Corte Superior, o fato de as informações serem fornecidas pelo consumidor no ato de uma compra ou até mesmo divulgadas em redes sociais não afasta a responsabilidade do gestor de previamente comunicar seu compartilhamento. A relatora do recurso (REsp n. 1758799-MG)[26], Ministra Nancy Andrighi, afirmou que, na hipótese de compartilhamento de informações sem prévia anuência, o dano moral é presumido, sendo desnecessário ao consumidor comprovar prejuízo. Esse julgamento se deu em torno da interpretação do inc. V do art. 5º. da Lei 12.414/11, que disciplina os bancos de dados para formação de histórico de crédito, mas não há dúvida de que pode ser aplicado, ainda que por analogia, a qualquer hipótese de compartilhamento não autorizado de dados pessoais, que estejam em poder de um controlador de sistema informatizado ou não.

Quem recebe os dados compartilhados indevidamente é igualmente responsável pela reparação devida aos titulares. Se o coletor original das informações não tem o direito de compartilhá-las, muito menos tem o

[26] REsp n. 1758799-MG, julgado em 12.11.19, DJe 19.11.19.

controlador destinatário de fazer uso delas, pela mesma razão de falta de autorização dos titulares. O princípio da finalidade resta desrespeitado pelo receptor dos dados de todo modo, já que os utiliza para outras finalidades, não autorizadas pelo titular. Compartilhamento de informações sem consentimento é ilegal. A ilegalidade se estende ao uso posterior dos dados transferidos sem o conhecimento do titular.

O Facebook tentou se livrar de responsabilização, no caso dos dados recebidos do *Zoom*, alegando que é dever das empresas que utilizam seu *kit* de desenvolvimento (*SDK*) informar aos usuários que estão compartilhando os dados com a plataforma, além de fornecer opção para desativar o compartilhamento[27]. Esse argumento não procede, pois cabe ao Facebook o dever de vigilância sobre os parceiros, de forma a evitar responsabilização por uso indevido de dados pessoais. A plataforma é o principal responsável pelo ressarcimento dos danos que ocorrem dentro do seu ecossistema, de desenvolvimento de aplicativos que utilizam suas "ferramentas de negócios" e outras tecnologias. Na condição de agente que controla a ferramenta central e os componentes que fazem funcionar esse "ecossistema", emerge como principal responsável pela reparação de danos à privacidade individual (do usuário). O dever de monitorar a atividade e comportamento dos aplicativos com os quais estabelece parceria ou tem algum tipo de integração tecnológica é da plataforma, até porque se reserva esse direito nos instrumentos contratuais que estabelece com as empresas parceiras. No documento "Termos de Uso" de suas "ferramentas de negócios", o próprio Facebook se concede o direito de realizar auditoria sobre a atividade dos aplicativos de empresas parceiras, desse

[27] Ver notícia referenciada na nota anterior.

modo: "Reservamo-nos o direito de monitorizar ou fazer auditorias ao teu nível de conformidade com os presentes Termos das Ferramentas de Negócios"[28]. Se nos acordos que celebra com seus parceiros o Facebook atribui-se o direito de supervisão sobre a atividade deles, ninguém mais do que ele próprio deve responder em caso de acidente ou desvio de conduta do outro contraente.

Não somente "metadados" eram transferidos por meio da integração (via *SDK*) entre o *Zoom* e o *Facebook*. A transferência de dados proporcionada pela ferramenta *SDK* não só tem o objetivo de permitir que o Facebook faça medição e compreensão da atividade do aplicativo parceiro, mas também o de identificar comportamentos que lhe permitam direcionar publicidade para os usuários. Com as informações que recebe sobre o funcionamento e atividade de aplicativos de programadores parceiros, o Facebook entrega aos seus anunciantes um perfil dos usuários, para que direcionem comerciais de produtos com base no interesse deles (usuários dos aplicativos parceiros). A configuração básica do *SDK* já inclui "um identificador de propaganda para que anunciantes direcionem comerciais de produtos com base no interesse dos usuários". Esse identificador é padrão para os parceiros do Facebook, que utilizam o seu SDK[29].

No documento "Termos de Uso" de suas "ferramentas de negócios", está escrito que o parceiro comercial (controlador de um *app* ou site) aceita partilhar dados pessoais com o Facebook. O mesmo documento esclarece que os *dados pessoais* transferidos por meio das "ferramentas de negócios" (que incluem SDKs) são os dados

---

[28] Ver redação do "Termos das Ferramentas de Negócios do Facebook", acessível em: https://www.facebook.com/legal/technology_terms

[29] Segundo notícia publicada em 27.03.20, pelo site *IG*, sob o título "Aplicativo de videoconferência Zoom envia dados dos usuários para o Facebook", acessível em: https://tecnologia.ig.com.br/olhar-digital/2020-03-27/aplicativo-de-videoconferencia-zoom-envia-dados-dos-usuarios-para-o-facebook.html

dos clientes e utilizadores de aplicações (*sites* ou *apps*), denominados de "Dados do Cliente", que podem incluir ***informações de contato***, aquelas que identificam pessoalmente os usuários (como nomes, endereços de e-mail e números do telemóvel), e **dados de eventos**, que são outras informações sobre os usuários e as ações que realizam dentro ou utilizando o aplicativo ou site parceiro (como visitas, início de sessões e compras dentro de aplicativos)[30].

Tal documento é uma espécie de contrato de adesão, ao qual o parceiro de negócios adere sem poder de discussão ou modificação das cláusulas preestabelecidas. Forçosamente, o parceiro é obrigado a repartir informações pessoais dos usuários de seu aplicativo ou site com o Facebook, a partir do momento em que instala a "ferramenta de negócios" que permite integração com a plataforma. Não tem como fugir do compartilhamento de dados que é imposto de forma unilateral.

---

[30] O trecho do ***Termos das Ferramentas de Negócios do Facebook***, nesse ponto, está redigido da seguinte maneira:
"Ao clicares em "Aceito" ou ao utilizares qualquer uma das Ferramentas de Negócios do Facebook, aceitas o seguinte:
1. Partilhar Dados Pessoais com o Facebook
   a. Podes utilizar as Ferramentas de Negócios do Facebook para nos enviares dados pessoais sobre os teus clientes e utilizadores ("**Dados do Cliente**"). Consoante os Produtos do Facebook que utilizas, os Dados do Cliente podem incluir:
      i. As "**Informações de Contacto**" consistem nas informações que identificam pessoalmente as pessoas, como nomes, endereços de e-mail e números de telemóvel que utilizamos apenas para fins de correspondência. Vamos converter as Informações de Contacto por hashing que nos enviares através de um píxel de javascript do Facebook para fins de correspondência antes da transmissão. Ao utilizares um píxel de imagem do Facebook ou outras Ferramentas de Negócios do Facebook, tu ou o teu fornecedor de serviços tem de converter as Informações de Contacto por hashing de uma forma especificada por nós antes da transmissão.
      ii. Os "**Dados de Eventos**" incluem outras informações que partilhas sobre os teus clientes e as ações que os mesmos realizam nos teus sites, apps ou lojas, como visitas aos teus sites, instalações das tuas apps e compras dos teus produtos."

Como se percebe, o compartilhamento de informações do *Zoom* para o *Facebook* envolveu **dados pessoais**, em grande volume e provavelmente durante muito tempo.

Essa não é a primeira vez em que o Facebook se vê no meio de denúncia de invasão de privacidade por causa da ferramenta *SDK*. Em fevereiro de 2019, o The *Wall Street Journal* publicou reportagem indicando que aplicativos compartilhavam informações sensíveis com o Facebook, através de um mecanismo analítico incluído no SDK[31].

Essa última ocorrência - recebimento de forma irregular de dados enviados pelo aplicativo *Zoom* - tem o mesmo potencial do escândalo da *Cambridge Analytica*. Trata-se de compartilhamento massivo de dados sensíveis (e sem conhecimento dos usuários), só que em sentido inverso. Naquele outro acontecimento, era o Facebook que repassava dados para os desenvolvedores de *apps*, os quais davam destinação diversa aos dados coletados. Agora, é o Facebook que recebe os dados e os utiliza para finalidades não autorizadas. Aquele escândalo, que chocou o mundo, obrigou o fundador do Facebook e seus executivos a comparecer perante comissões parlamentares e reformular completamente suas práticas e a política de privacidade. Somente como multa à agência reguladora do comércio e de proteção ao consumidor (*FTC-Federal Trade Comission*) dos Estados Unidos, o Facebook teve que pagar 5 bilhões de dólares[32]. Quanto terá que desembolsar para reparar os danos causados pelo "Zoomgate"?

---

[31] Ver reportagem publicada no dia 22.02.19, acessível em: https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636

[32] Ver reportagem publicada pelo jornal El País, em 13.07.19, acessível em: https://brasil.elpais.com/brasil/2019/07/12/economia/1562962870_283549.html

Recife, 10 de abril de 2020.