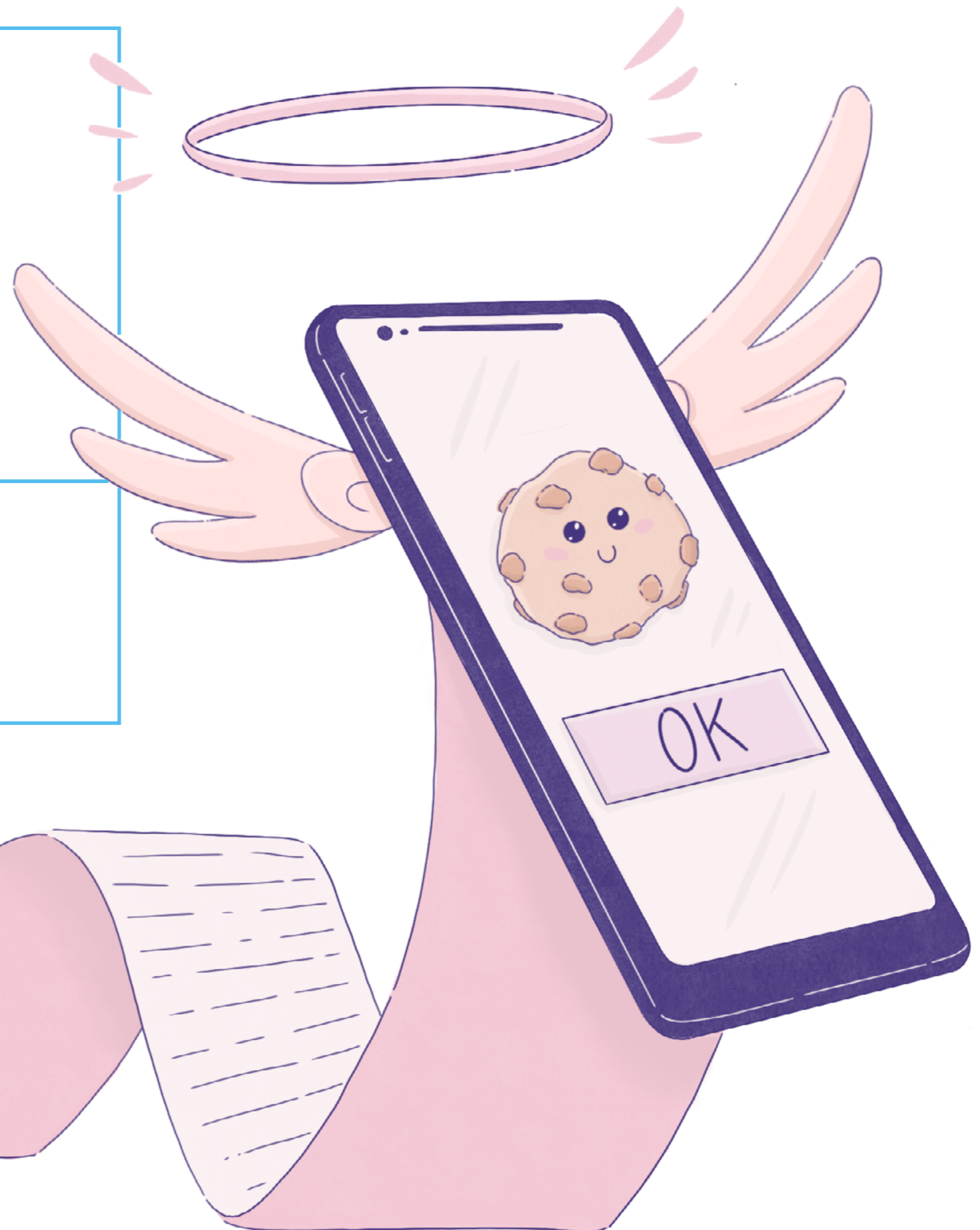


Aplicação da Lei de Proteção de Dados Pessoais

um estudo de caso de apps de empresas com modelo de negócio baseados em dados



FICHA TÉCNICA

Aplicação da Lei de Proteção de Dados Pessoais: um estudo de caso de apps de empresas com modelo de negócio baseado em dados

Tradução da pesquisa “Aplicación de la Ley de Protección de Datos Personales en Brasil: estudio de caso de algunas empresas con modelo de negocio basado em datos” escrita por Kimberly Anastácio, Bruna Santos e Joana Varon, realizada pela Coding Rights como parte da publicação “Festín de Datos: Empresas y datos personales en América Latina”, por Vivian Newman Pont, Daniel Ospina-Celis e Juan Carlos Upegui.

Autoras

Kimberly Anastácio, Bruna Santos e Joana Varon

Coordenadora do Projeto - Coding Rights

Joana Varon

Coordenador do Projeto - DeJusticia

Daniel Ospina

Design

Clarote

Data da Publicação

Rio de Janeiro, Junho 2020.

Publicação

Coding Rights | contato@codingrights.org



Esse texto está disponível para download em www.codingrights.org

ÍNDICE

INTRODUÇÃO // 4

I. SELEÇÃO DAS EMPRESAS COM MODELO DE NEGOCIO BASEADO EM DADOS // 7

1. Empresa Gafam: Amazon Prime Video // 7
2. Empresa intermediária: Ifood // 8
3. Start-up: Social Miner // 9
4. Empresa estabelecida: Magazine Luiza // 9

II. CARACTERIZAÇÃO DA FORMA DE OPERAR DAS EMPRESAS // 12

1. Fonte dos Dados // 12
2. Tratamento e Finalidades // 19
3. Relação com as empresas GAFAM // 25
4. Casos de violações de privacidade relacionados à marca // 27

III. AVALIAÇÃO DO REGIME JURÍDICO DE PROTEÇÃO DE DADOS PESSOAIS PARA ABORDAR AS DINÂMICAS DAS EMPRESAS ANALISADAS // 29

1. Regime jurídico de proteção de dados no Brasil // 29
2. Pontos principais da Lei de Proteção de Dados no que diz respeito às práticas das quatro empresas selecionadas // 31
 - a) Finalidade, consentimento e compartilhamento com terceiros // 32
 - b) Uso de cookies // 35
 - c) Relação com GAFAM pode decorrer em tratamento não autorizado de dados sensíveis? // 37
 - d) Dispositivos vagos sobre segurança e sigilo dos dados // 40

e) Direito de acessar com facilidade, corrigir ou deletar informações // 42

f) Prática de profiling e potencial de discriminar por algoritmos // 44

IV. AVALIAÇÃO DA ADEQUAÇÃO DO REGIME JURÍDICO PARA AS DINÂMICAS PRÓPRIAS DA ERA DIGITAL // 46

V. AVALIAÇÃO DA CAPACIDADE DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS PARA LIDAR COM AS EMPRESAS SELECIONADAS // 48

VI. CONCLUSÃO E RECOMENDAÇÕES // 53

REFERÊNCIAS // 58

ANEXOS - VERSÃO DOS TERMOS DE USO E POLÍTICAS DE PRIVACIDADE ANALISADAS PARA ESSA PESQUISA // 65

Anexo I. Política de Privacidade - iFOOD // 66

Anexo II. Termos e Condições - iFOOD // 80

Anexo III. Política de Privacidade - Social Miner // 83

Anexo IV. Política de Cookies - Social Miner // 91

Anexo V. Política de Privacidade - Magazine Luiza // 93

Anexo VI. Termos de Uso do Amazon Prime Video // 96

Anexo VII. Amazon Privacy Notice // 104

Anexo VIII. Termos e Condições de uso - específico para assinatura do Prime Video pelas clientes Vivo // 112

Anexo IX. Termo de Tratamento de Dados Pessoais da Telefônica // 114

INTRODUÇÃO

A presente pesquisa foi conduzida pela Coding Rights em parceria com o Centro de Estudios de Derecho, Justicia y Sociedad (Dejusticia), que coordenou a publicação “Festín de Datos: Empresas y datos personales en América Latina”, uma pesquisa comparativa entre Colômbia, Chile, México e Brasil sobre a implementação das suas respectivas leis de proteção de dados pessoais.

Como parceiros para realizar o estudo no Brasil, analisamos as políticas de privacidade e os termos de uso de aplicativos de serviços online¹ que atendem ao território brasileiro para averiguar como eles se enquadram no que dispõe a lei brasileira sobre proteção de dados pessoais.

Seguindo metodologia de análise comparativa definida para o estudo, selecionamos para a análise os serviços oferecidos por quatro empresas com modelos de negócio baseados em dados (as chamadas EMNBD), sendo cada uma representante das seguintes categorias:

Grandes empresas de Internet: selecionamos a “Amazon Prime Video”, serviço de streaming da Amazon, representando serviço de uma empresa integrante do grupo GAFAM, acrônimo para o grupo de cinco grandes empresas estadunidenses que lideram o mercado mundial de aplicações na Internet - Google, Apple, Facebook, Amazon e Microsoft.

Empresas intermediárias: escolhemos a “Ifood”, empresa brasileira de entrega de comida, que apesar de recente, já alcançou posição de destaque no mercado do país, sendo o número 1 em downloads na categoria “food & drink”, e inclusive já expandiu suas operações para fora do país.

Start-ups: para essa categoria selecionamos a “Social Miner, empresa que auxilia outras empresas na otimização de marketing digital e beneficiária de programas de aceleração de grandes empresas como Google e Oracle. A start-up integra o

¹ Vale destacar que a presente pesquisa analisou os termos de usos e políticas de privacidade os serviços em questão durante os meses de agosto e outubro de 2019. No caso do Ifood, a análise foi dos termos de uso para clientes da plataforma, e não os referentes ao App do entregador: <https://entregador.ifood.com.br/termosdeuso/>. Já no caso do Amazon Prime Vídeo, a pesquisa levou em consideração os termos de uso referentes à 2019, no entanto, no dia 1o de janeiro de 2020 a empresa publicou novos termos de uso: https://www.primevideo.com/help/ref=atv_hp_nd_nav?nodeId=G202095490

ranking elaborado em 2018 pela revista "Grandes Empresas e Grandes Negócios" como uma das "100 start-ups para ficar de olho" (do inglês "100 Startups to Watch") no Brasil.

Empresas estabelecidas: por fim, para essa categoria selecionamos o "Magazine Luiza", empresa de varejo que passou a fazer vendas pela Internet. Diferente das categorias anteriores, essa empresa não tinha como foco do modelo de negócios os dados pessoais, mas vem mudando suas práticas para incorporar análises de dados.

Após a coleta dos dados e escrita da análise inicial, realizamos um encontro com representantes dos setores interessados nas políticas de Internet para debater os achados da pesquisa. O artigo se divide em quatro seções. A primeira delas expõe os critérios de seleção das quatro empresas analisadas e identifica nos termos de uso e políticas de privacidade dessas empresas quatro aspectos principais: (a) a fonte dos dados coletados, (b) o tratamento dos dados, (c) a finalidade de seu uso e (d) o relacionamento das empresas e dos dados coletados com as empresas do grupo GAFAM.

Em seguida, analisamos como as práticas dessas empresas se encaixam no regime jurídico de proteção de dados no Brasil. Para tanto, observando as práticas das empresas selecionadas, detalhamos pontos que podem ser contrastantes como o que diz a Lei de Proteção dos Dados Pessoais (LGDP) e outros dispositivos referentes à proteção de dados e da privacidade, como o Código de Defesa do Consumidor, o Marco Civil da Internet e à própria Constituição Federal. Diante desse marco regulatório, avaliamos se o que temos hoje como marco regulatório para a proteção dos dados pessoais e se o que temos previsto como forma de funcionamento da Autoridade Nacional de Proteção de Dados Pessoais (ANPD), entidade responsável pela supervisão da aplicação da lei brasileira, responderiam às práticas das empresas elencadas, principalmente no que diz respeito à capacidade de regulação, supervisão, controle e sanção da autoridade.

Por fim, apresentamos conclusões e recomendações para que a forma de operar das EMNBD se alinhe cada vez mais com os princípios e a regulação de proteção de dados pessoais no país, sobretudo considerando a necessidade de as empresas estarem alinhadas com a recém aprovada lei (LGDP), que entrará em vigor em agosto de 2020.

No contexto de hiper digitalização introduzido pela pandemia de Covid-19 e a necessidade de isolamento social para contê-la, os serviços estudados na presente pesquisa tem assumido um papel cada vez mais forte em nossas vidas. E, com um maior número de pessoas confinadas em casa, a demanda requerida destes aplicativos e serviços é maior e fomenta um melhor planejamento das empresas em termos de cronogramas, aumento de mão de obra no caso dos apps de entrega e,

diminuição da qualidade dos vídeos para atender o aumento expressivo de público, no caso de serviços de acesso condicionado como o Amazon Prime Video. Por fim, isso também significa uma coisa: há mais dados do que nunca circulando por aí. Pensando nisso, torna-se mais necessária ainda a análise de práticas e políticas de privacidade realizada pela presente pesquisa.

I. SELEÇÃO DAS EMPRESAS COM MODELO DE NEGOCIO BASEADO EM DADOS

1. Empresa Gafam: Amazon Prime Video

A Amazon, empresa integrante do grupo GAFAM, foi a nossa escolhida. Neste estudo vamos analisar o serviço de vídeo sob demanda Amazon Prime Video, bem como as especificidades de sua oferta casada com a Vivo, concessionária de telefonia brasileira integrante do grupo Telefônica. Desde setembro de 2018, a operadora de telefonia Vivo, da empresa Telefônica, passou a disponibilizar em parceria com a Amazon, o serviço de vídeo streaming Amazon Prime Video. O Amazon Prime chegou ao Brasil efetivamente a partir de setembro de 2019, quando o presente estudo estava em andamento. Anteriormente, desde setembro de 2018, a operadora de telefonia Vivo, a empresa Telefônica, tinha uma parceria com a Amazon para fornecer o serviço de transmissão de vídeo Amazon Prime Video a seus clientes. Portanto, analisamos os documentos e políticas em vigor antes de setembro de 2019, quando o serviço foi realizado em conjunto com a Vivo. Neste caso, a empresa oferece 90 dias de acesso gratuito, depois cobra R\$7,90 nos seis primeiros meses e, no mês seguinte, passa a cobrar R\$14,90 por mês². Mas para assinar, é preciso ser cliente Vivo, ou de plano celular ou de banda larga. A Amazon também fornece diretamente o plano no Brasil, mas dá apenas 7 dias de gratuidade, depois o plano também custa R\$7,90 por mês nos seis primeiros meses, e depois passa a ser cobrado R\$14,90 mensais³.

Além de achar interessante essa parceria com a Vivo no que diz respeito à proteção de dados, também achamos importante analisar o Amazon Prime Video em função da disputa entre Google e Amazon a respeito do serviço, depois de meses de retaliações, os dois gigantes chegaram num acordo e desde junho de 2019 o serviço está disponível para o ChromeCast⁴.

2 VIVO. Vivo para sua casa. Disponível em: https://www.vivoparasuacasa.com.br/amazonprimevideo/?gclid=EAlalQobChMlIba8weX_4wIVIIaRCh3epwrjEAAYASAAEgKRIVD_BwE

3 AMAZON. Amazon Prime Video. Disponível em: <https://www.primevideo.com/>

4 GARTENBERG, C. (2019). YouTube is back on the Fire TV, and Prime Video launches on Chromecast starting today. The Verge. Disponível em: <https://www.theverge.com/2019/7/9/20686773/youtube-fire-tv-prime-video-chromecast-amazon-google-launch-today-available>

2. Empresa intermediária: Ifood

Empresa de capital fechado, fundada em 2011, e hoje presente em mais de 200 cidades⁵ do país além de México, Colômbia e Argentina, o Ifood é uma plataforma de delivery de comida. O serviço, oferecido em versão web e aplicativos para iOS, Android e Windows Phone, conta com quase 600 mil pedidos por dia no Brasil originados pelos seus 12 milhões de usuários ativos⁶. A Empresa ainda possui um produto chamado iFoodLabs, laboratório de inovação focado em aplicar visão de negócio em idéias que unem tecnologia e alimentação. Por meio de dados de mercado, experiências, casos de uso dos clientes, entrevistas com stakeholders e especialistas, a idéia do laboratório é utilizar metodologias de design para criar soluções para o mercado de delivery e cadeia produtora de alimentos; o laboratório gerou produtos como o SpoonRocket⁷ e iFoodNext, divisão concentrada em desenvolver software e serviços focados em demandas de donos de restaurantes. A empresa ainda possui uma plataforma chamada iFood Shop⁸, que conecta os restaurantes a fornecedores de embalagens e insumos.

Criada por Felipe Fioravante e Patrick Sigrist, a startup tem recebido aportes de empresas como a Móvile, que investiu 5.5 milhões de reais em 2013⁹ e 125 milhões de reais (juntamente com a empresa Britânica Just Eat) em 2015. Em novembro de 2018, a Móvile anunciou que o iFood receberia investimento de US\$ 500 milhões¹⁰ - o equivalente a R\$ 1,9 bilhão - o que representou o maior aporte privado em empresa privada de tecnologia no Brasil. A idéia do aporte foi a de ampliar a atuação do iFood no país e dobrar os números de restaurantes (atualmente cerca de 66 mil) e cidades atendidas (500 municípios)¹¹.

O Ifood ocupa a 23^a posição entre os aplicativos mais baixados da Play Store. O aplicativo conta com mais de 10 milhões de downloads e é o mais baixado de toda a Play Store considerando a categoria “Comer e beber”.

5 IFOOD. Cidades Atendidas. Disponível em: <https://www.ifood.com.br/cidades-atendidas>

6 DAROIT, G. (2019). iFood quer seguir entregando crescimento. Jornal do Comércio. Disponível em: https://www.jornaldocomercio.com/_conteudo/cadernos/empresas_e_negocios/2019/05/685035-ifood-quer-seguir-entregando-crescimento.html

7 SPOONROCKET. Disponível em: <https://www.spoonrocket.com.br/>

8 BELLONI, L. (2018). Como o iFood se tornou o maior aplicativo de delivery de comida da América Latina. Huffington Post. Disponível em: https://www.huffpostbrasil.com/2018/04/18/como-o-ifood-se-tornou-o-maior-aplicativo-de-delivery-de-comida-da-america-latina_a_23414651/

9 ZUINI, P. (2013). Móvile investe R\$ 5,5 milhões na iFood. Exame. Disponível em: <https://exame.abril.com.br/pme/movile-investe-r-5-5-milhoes-na-ifood/>

10 BRIGATTO, G. (2018). Móvile investe US\$ 500 milhões no iFood e planeja criar líder global. Valor Econômico. Disponível em: <https://www.valor.com.br/empresas/5983273/movile-investe-us-500-milhoes-no-ifood-e-planeja-criar-lider-global>

FREITAS, T. (2019). iFood registra 17,4 milhões de pedidos no mês de março. Startse. Disponível em: <https://www.startse.com/noticia/startups/63248/ifood-atinge-a-marca-174-milhoes-de-pedidos-no-mes-de-marco>

3. Start-up: Social Miner

A empresa figura em várias listas de startups que merecem atenção no país, tendo chamado a atenção de programas de aceleração de startups liderados por empresas como Oracle¹² e Google¹³. A empresa não conta com um aplicativo, no entanto desenvolveu sua própria plataforma de direcionamento de propaganda online.

Criada em 2014, declara ter o objetivo de “aproximar marcas e pessoas da tecnologia e melhorar as respectivas performances online por meio da utilização de tecnologias de Inteligência Artificial e Big Data”¹⁴. A Empresa identifica práticas de consumo, perfis de consumidores e metodologias de engajamento online para marcas por meio de uma base de dados capaz de identificar a “etapa da jornada em que um consumidor está e sua intenção de compra”¹⁵ para que as empresas consigam realizar propaganda direcionada/engajamento com aqueles consumidores que eventualmente não comprariam seus produtos.

Assim, a Social Miner não possui um aplicativo e coleta dados de indivíduos que trafegam por páginas de seus clientes na Internet. É uma empresa cujos produtos não tem interação com os usuários finais, uma vez que oferece estratégias de engajamento e marketing digital para empresas, ou as contratantes. De acordo com o próprio site da empresa, a Social Miners oferece uma plataforma que permite às empresas contratantes - dentre elas Avon, Asus, Sephora Brasil, Natura, Extra e Wine.com.br¹⁶ - uma melhor compreensão dos contextos e linguagens ideais para incentivar consumidores indecisos, segmentar seus dados e criar campanhas personalizadas.

4. Empresa estabelecida: Magazine Luiza

A Magazine Luiza é uma empresa especializada no setor de varejo cuja estratégia digital chamou a atenção por possuir produtos como uma bot, a Lu, com canal no youtube, programas que incentivam a produção de conteúdo de suas lojas

12 SOCIAL MINER. (2018). Social Miner no Oracle Startup Cloud Accelerator. Blog da Social Miner. Disponível em: <http://blog.socialminer.com/people-marketing/social-miner-no-oracle-startup-cloud-accelerator/>

13 FREITAS, T. (2019). As 8 startups brasileiras de machine learning que serão aceleradas pelo Google. Startse. Disponível em: <https://www.startse.com/noticia/startups/61939/8-startups-brasileiras-launchpad-accelerator>

14 SOCIAL MINER. Sobre Nós. Disponível em: <https://socialminer.com/sobre-nos.html>

15 Portal da Social Miner. Disponível em: <https://socialminer.com/>

16 SOCIAL MINER. Cases de Sucesso. Disponível em: <https://socialminer.com/>

para o Facebook e pelo fato de seu aplicativo contar com mais de 10 milhões de instalações na Play Store Brasil¹⁷ e ocupar a 2ª posição de aplicativos de compra mais baixados na App Store Brasil¹⁸.

Fundada em 1957 em Franca, São Paulo, a marca possui mais de 900 lojas físicas, 12 centros de distribuição espalhados por 17 estados brasileiros¹⁹. E oferece produtos dos setores de móveis, eletrodomésticos, eletroeletrônicos, presentes, brinquedos, hobby e lazer, informática e telefonia tanto nas lojas físicas quanto no site e aplicativo. O Magazine Luiza introduziu o conceito de Lojas virtuais em 1991, quando suas lojas não possuíam produtos físicos²⁰. A época, as vendas eram realizadas em terminais eletrônicos e a entrega do produto ocorria até 48h depois da aquisição; o modelo de loja virtual continua em exercício pela marca, o que permite a existência de lojas sem estoques físicos ou mostruários. Em 2013, a companhia ainda introduziu sua assistentes eletrônicas de vendas, a Lu, criada para instruir os usuários a utilizar produtos conectados, melhorar a navegação pelo site²¹ e, assim, contribuir para a inclusão digital dos clientes²². A mesma avatar digital ajudou a aumentar as vendas online em 56% no primeiro semestre de 2017²³ e ainda conta com um canal de Youtube²⁴ com 1.6 milhões de seguidores.

A empresa possui estratégias bem representativas para o desenvolvimento de sua plataforma digital - além dos já mencionados aplicativo, site, lojas virtuais, canal no Youtube e avatar - o Magazine Luiza também foi pioneira na operação de varejo omni-channel do Brasil²⁵. A operação de Omnichannel permite que vários canais de venda usassem a mesma infraestrutura (centros de distribuição, contabilidade, marketing). Algumas estratégias digitais da companhia merecem atenção,

17 Google Play Store. Disponível em: https://play.google.com/store/apps/details?id=com.luizalabs.mlapp&hl=pt_BR

18 App Store. Disponível em: <https://apps.apple.com/br/app/magazine-luiza-comprar-online/id891130066>

19 MAGAZINE LUIZA. Quem Somos. Disponível em: <https://ri.magazineluiza.com.br/ShowCanal/Quem-Somos?urUqu4hANldyCLgMRgOsTw==>

20 GAZZONI, M E CRUZ, P. (2011). Luiza Trajano: do balcão da loja dos tios a ministra do governo. Último Segundo - iG. Disponível em: <https://ultimosegundo.ig.com.br/politica/luiza-trajano-do-balcao-da-loja-dos-tios-a-ministra-do-governo/n1597158849986.html>

21 CALADO, C. (2018). Magazine Luiza – entrevista com o time responsável pela criação da Lu. Medium Bots Brasil. Disponível em: <https://medium.com/botsbrasil/magazine-luiza-entrevista-com-o-time-respons%C3%A1vel-pela-cria%C3%A7%C3%A3o-da-lu-8fc987fbafad>

22 FRAGA, N. (2018). "Temos de ajudar o consumidor na inclusão digital", diz Trajano, do Magazine Luiza. Época Negócios. Disponível em: <https://epocanegocios.globo.com/Empresa/noticia/2018/02/fabio-coelho-do-google-e-luiza-trajano-do-magazine-luiza-conversam-sobre-inclusao-digital.html>

23 BLOOMBERG. (2017), Magazine Luiza usa Tinder pra ampliar vendas e tem alta de 2000%. Jornal O Globo. Disponível em: <https://oglobo.globo.com/economia/magazine-luiza-usa-tinder-pra-ampliar-vendas-tem-alta-de-2000-21705034>

24 MAGAZINE LUIZA. Canal da Lu - Magalu. Youtube. Disponível em: <https://www.youtube.com/user/MAGAZINELUIZACOM>

25 RICCIARDI, A. (2016). Como Frederico Trajano está mudando os rumos do Magazine Luiza. Forbes. Disponível em: <https://forbes.uol.com.br/negocios/2016/07/como-frederico-trajano-esta-mudando-os-rumos-do-magazine-luiza/>

como o Programa Maga Local, o Marketplace e, inclusive, ação de marketing no tinder que concedia descontos especiais para usuários do aplicativo que dessem match com o perfil da Lu²⁶. Ainda sobre o Maga Local e o Marketplace da empresa, vale destacar que o primeiro visa incentivar que as lojas tenham fanpages próprias no facebook, bem como autonomia para produzir conteúdo; já o marketplace da empresa, lançado em 2016, hoje permite que sejam ofertados no aplicativo e site do Magazine Luiza produtos de mais de 500 outras empresas e representa um quarto das vendas digitais da empresa²⁷.

Em matéria de outubro de 2017²⁸, o presidente da Magazine Luiza, Frederico Trajano, apontou que a empresa pretendia enfrentar a expansão da operação brasileira da Amazon com possíveis reforços aos pontos físicos e da integração de loja online com loja física. A época, o comércio eletrônico representava 30% da receita do Magazine Luiza, algo como 4 bilhões de reais, e o aplicativo já contava com 7 milhões de acessos mensais²⁹.

26 BLOOMBERG. (2017), Magazine Luiza usa Tinder pra ampliar vendas e tem alta de 2000%. Jornal O Globo. Disponível em: <https://oglobo.globo.com/economia/magazine-luiza-usa-tinder-pra-ampliar-vendas-tem-alta-de-2000-21705034>

27 MAGAZINE LUIZA. (2019). E-commerce do Magazine Luiza cresce 56% no segundo trimestre Em menos de três anos, faturamento do Marketplace chega a ¼ das vendas digitais. Release. Disponível em: <https://ri.magazineluiza.com.br/Download/magalurelease2T19--1-?=Iart1882KdnmVEwBwRdEmQ=&idcanal=rqFYRysdRDkTGGc93mpXJg==>

28 MANZONI JR, R. (2017). Como o Magazine Luiza pretende enfrentar a Amazon? Istoé Dinheiro. Disponível em: <https://www.istoedinheiro.com.br/como-o-magazine-luiza-pretende-enfrentar-amazon/>

29 IDEM.

II. CARACTERIZAÇÃO DA FORMA DE OPERAR DAS EMPRESAS

1. Fonte dos Dados

Ofertas de emprego na Amazon Prime Video destacam como a empresa pretende “moldar o futuro do entretenimento em vídeo” por meio da contratação de pessoas para cargos como Business Intelligence Engineers, com a missão de “descobrir como consumidores assistem vídeos na Amazon” e “trabalhar em uma das maiores bases de dados de consumidores do mundo”³⁰. Outro cargo, de líder de uma equipe de engenheiros e cientistas de dados destaca que a equipe é responsável por “definir e entregar medições de comportamento e marketing de clientes”³¹. Não há dúvidas de que a coleta e tratamento de dados pessoais de seus consumidores estão no centro desse, entre muitos outros, negócio da Amazon.

No Brasil, o que nos chamou atenção particular foi que esses serviços são ofertados também em parceria com a Vivo. Empresa de telefonia móvel que, assim como várias outras, inclusive já foi alvo de inquérito³² por suspeita de uso de dados pessoais.

Segundo site da Vivo, quem já é consumidor de seus planos de telefonia celular só precisa enviar um SMS com a palavra AMAZON para contratar o Amazon Prime Video. A plataforma está até fazendo parcerias para produção de conteúdo brasileiro³³. O consumidor desse serviço fica então sujeito tanto aos termos de uso da Vivo³⁴ como da Amazon Prime Video³⁵, em caso de conflito, a Vivo declara que prevalecem seus termos.

30 LINKEDIN. Head of Subscription Video Analytics, Prime Video US. Amazon Job post at LinkedIn. Disponível em: <https://www.linkedin.com/jobs/view/head-of-subscription-video-analytics-prime-video-us-at-amazon-1094636760/>

31 HIGA, P. (2019). Fim da briga: YouTube volta ao Fire TV e Prime Vídeo estreia no Chromecast. Tecnoblog. Disponível em: <https://tecnoblog.net/297901/youtube-volta-fire-tv-prime-video-chromecast/>

32 LUNA, D. (2018). MP do DF abre inquérito contra Vivo por suspeita de uso de dados pessoais. O estado de S. Paulo. Disponível em: <https://link.estadao.com.br/noticias/empresas,mp-do-df-abre-inquerito-contra-vivo-por-suspeita-de-uso-de-dados-pessoais,70002253400>

33 MEIO E MENSAGEM. (2018). Amazon Prime Video e Viacom anunciam conteúdo original. Disponível em: <https://www.meioemensagem.com.br/home/ultimas-noticias/2018/11/14/viacom-negocia-series-para-amazon-prime-video.html>

34 VIVO. TERMOS E CONDIÇÕES DE USO – ESPECÍFICO PARA ASSINATURA DE PRIME VIDEO PELOS CLIENTES VIVO. Disponível em: http://ws.mobile.terra.com/Descargas/Storage/000000000/062000/062250/Terms62250_PT_20181008133419.pdf

35 AMAZON. (2019) Termos de Uso do Amazon Prime Video. Disponível em: <https://www.primevideo.com/region/na/help?nodeId=202095490>

Como nesse caso temos no mínimo duas empresas contratantes, as fontes de dados vêm tanto do que dispõe o Centro de Privacidade da Vivo³⁶, como dos Termos de Uso³⁷ e Aviso de Privacidade³⁸ da Amazon.

Nos termos de Uso da Amazon Prime Video, linkados no contrato de assinatura do serviço com a Vivo, ou ao buscar diretamente na Amazon, quando queremos contratar o serviço diretamente com a empresa estrangeira, encontramos informações de que o Video Market place da Amazon tem diferentes fornecedores e, portanto, distintos termos e políticas aplicáveis que variam de região para região. Entre os países da América Latina, apenas o México aparece listado explicitamente. Consumidores brasileiros ficam enquadrados na categoria “Estados Unidos e todos os outros países não indicados acima”, cujo fornecedor é a sede da Amazon em Seattle. Os termos aplicáveis e notificações legais são as seguintes, alguns disponíveis apenas em inglês:

- *Amazon Prime Video Terms of Use (disponível em PT)*
- *Amazon Prime Video Usage Rules (disponível em PT)*
- *Condition of Use (disponível apenas em ING)*
- *Privacy Notice (disponível apenas em ING)*
- *Interest-Based Ads Policy (disponível apenas em ING)*
- *Twitch Terms of Service (disponível apenas em ING)*

Nos termos de uso do Amazon Prime Video, temos disposto na seção denominada “Software” que “o serviço poderá fornecer à Amazon informações relativas ao seu uso e performance, assim como informações referentes aos dispositivos que utilizam o serviço e software”³⁹. Incluem-se aí informações sobre a maneira em que estamos consumindo o conteúdo digital da plataforma. Ou seja, qual conteúdo baixamos, acessamos ou estamos assistindo, e quando.

Os documentos de termos de uso e regra de uso do Amazon Prime Video nada mais dispõe sobre proteção de dados pessoais do que o disposto acima, mas afirmam que essas informações estão sujeitas ao Aviso de Privacidade da Amazon,

36 VIVO. Centro de privacidade. Disponível em: https://www.vivo.com.br/portalweb/appmanager/env/web?_nfls=false&_nfpb=true&_pageLabel=vivoVivolnstPrivacidadePage&WT.ac=portal.amarca.privacidade&#

37 AMAZON. (2019) Termos de Uso do Amazon Prime Video. Disponível em: <https://www.primevideo.com/region/na/help?nodeId=202095490>

38 AMAZON. (2017). Amazon Privacy Notice. Disponível em: <https://www.amazon.com/gp/help/customer/display.html?nodeId=468496>

39 VIVO. Centro de privacidade. Disponível em: <https://www.vivo.com.br/portalweb/appmanager/env/web?>

que, por sua vez, está disponível apenas em inglês, mesmo para quem contrata o serviço no Brasil.

Nesses documentos destacamos que a Amazon determina que pode coletar os seguintes tipos de dados e informações sobre nós: a) informações que compartilhamos sobre nós mesmos; b) “informação automatizada”, onde menciona o uso de cookies; c) informações sobre nossos dispositivos, inclusive a confirmação de recebimento/leitura de emails de comunicação que envia para seus clientes; e, por fim, d) “informações de outras fontes”, incluindo informações que vão desde endereço de entrega, dados de compras, de visualização de páginas, resultados de busca ou termos utilizados em buscas feitas via Alexa e até mesmo informação de histórico de crédito de bureaus de crédito.

Já o Centro de Privacidade da Vivo descreve que coleta informações sobre: a) nossos dados cadastrais, como nome, endereço, CPF e outros informados no contrato; b) volume de dados trafegados na internet; c) histórico de uso dos produtos e serviços contratados, o que, segundo a empresa, não envolve registros de apps que não sejam da vivo, nem de atividades nas redes sociais; d) histórico de chamadas e SMS recebidas; e) informações contábeis e fiscais e dados de atendimento ao cliente.

No caso do Ifood, de acordo com a política de privacidade, os dados coletados e tratados pela empresa concentram-se em três fontes principais. A primeira são os dados proporcionados pelo próprio usuário/cliente. Ao se cadastrar, o usuário já se compromete a fornecer informações como nome, endereço, CPF, email, telefone e data de nascimento. Com o uso contínuo do aplicativo ou site, a empresa ainda coleta dados sobre o comportamento do usuário na plataforma, traçando um histórico de suas compras e buscas dentro do aplicativo, tempo gasto no aplicativo e afins. Há, ainda, a coleta de informações sobre dados de pagamento, com número e validade de cartões de crédito do cliente. Parte vital para o funcionamento do aplicativo é a coleta de dados de localização, que podem ser fornecidos pelo usuário ou coletados pelo GPS e redes móveis do celular cadastrado. Segundo política de privacidade, tal informação “para fins da lei nº 12.965 de 2014 (Marco Civil da Internet), ou qualquer lei que venha substituí-la, (...) será considerada como dado cadastral”.

A segunda fonte principal são os dados compartilhados por sócios estratégicos. Nesse caso, há a possibilidade do cliente fazer seu login diretamente com a conta do Facebook, permitindo que o Ifood colete dados de tal rede associados diretamente à identidade do cliente, como nome, gênero, idade. Já a terceira fonte de dados é o que se chama de webtracking e informações de dispositivo. Segundo a política de privacidade, o Ifood pode coletar informações automaticamente sobre os dispositivos usados para utilização do aplicativo, incluindo “endereços IP, tipo de navegador e idioma, provedor de serviços de Internet (ISP), páginas de consulta e saída, sistema operacional, informações sobre data e horário, dados sobre a sequência de cliques, fabricante do dispositivo, operadora, modelo, redes Wi-Fi, número de telefone”.

A política de privacidade do Ifood também declara que informações sobre as atividades dos usuários na Web ou no aplicativo serão consideradas como dados agregados e informações não-pessoais. A política de privacidade também dispõe que “a idade do indivíduo, preferências individuais, idioma, CEP e código de área” também são consideradas informações não-pessoais, desde que não sejam combinados com dados pessoais do indivíduo em questão.

Quanto à Social Miner, em uma matéria lançada no site “Projeto Draft”⁴⁰, a empresa foi citada como uma promissora iniciativa que “usa inteligência artificial, perfil social e comunicação para automatizar campanhas de marketing digital com um alto grau de personalização”. A Social Miners alega introduzir o fator humano nas tecnologias já desenvolvidas para marketing digital, no conceito que eles definem como “people marketing” - ou entregar ao usuário um direcionamento feito exclusivamente para ele. Ainda de acordo com o mesmo artigo, o engajamento da Social Miners ocorre da seguinte maneira:

“Imagine que você está navegando em um e-commerce que contrata a Social Miner e resolve sair do site. Ao notar o movimento do cursor do mouse para fora da tela, o algoritmo percebe que você não iria realizar a compra naquele momento e oferece um benefício para você ficar em contato com a marca, que pode ser um cupom ou até mesmo acesso a dicas exclusivas. Também pode ser um pop-up (que não impede que você feche a página).

Quando o usuário decide fazer o login via Facebook, a plataforma obtém dados que tornam possível chamá-lo pelo nome e direcionar o conteúdo de acordo com sua cidade, sexo e faixa etária, por exemplo. A partir do momento do cadastro, o algoritmo da Social Miner começa a monitorar o perfil de navegação no site para entender o comportamento do usuário: que produtos já viu, se já fez alguma compra naquela loja etc.

Depois de coletar essas informações, é a hora de falar com o usuário, na hora certa.”⁴¹

Ante o disposto acima, fica claro que a plataforma de direcionamento de conteúdo oferecida pela Social Miner é alimentada

40 SOUZA, B. (2016). Como a Social Miner usa inteligência artificial, mas também gente, para inovar no marketing digital. Projeto Draft. Disponível em: <https://projetodraft.com/como-a-social-miner-usa-inteligencia-artificial-mas-tambem-gente-para-inovar-no-marketing-digital/>

41 IDEM.

por dados de navegação dos usuários, além dos dados de login em plataformas como Facebook. Importante mencionar que, com os dados coletados e serviços oferecidos, a startup publicou o relatório chamado **“O comportamento do consumidor Online em 2018”**⁴² que contém análise de perfil de consumo de 35 milhões de pessoas cadastradas em sua base de dados, bem como estatísticas de performance de sites de e-Commerce.

O “people marketing” - conceito desenvolvido pela Social Miners - tem chamado a atenção de programas de aceleração de startups liderados por empresas como Oracle e Google. A empresa, com 5 anos de existência, também conta com investimento de fundos como Canary, Wayra (Grupo Telefônica) e Indicator Capital.

A empresa afirma atuar em concordância com o regulamento europeu, além de prezar pela segurança de dados e privacidade dos usuários⁴³. Por isso, a ferramenta lista uma série de oito direitos dos usuários afetados pela empresa⁴⁴. Tal lista inclui, entre outros, o direito de ser informado sobre quais dados são coletados e de demandar ajustes na coleta, o direito de proibir a coleta de novos dados e o direito de “contestar decisões feitas por meio automatizados, ou elaboração de perfis, se tais decisões tiverem o poder de produzir efeitos jurídicos para si, ou outro efeito igualmente significativo”⁴⁵.

Em relação à coleta de dados, para o contato pró-ativo do time de vendas, a Social Miner coleta informações como nome, e-mail, telefone, site da empresa, setor ou categoria de negócio e tráfego do site da empresa “sempre que um visitante fizer download de algum material educativo, realizar um cadastro no nosso site ou participar de algum webinar ou evento organizado pela Social Miner”⁴⁶.

Além disso, sempre que um usuário navega no site da empresa, a visita é transformada em dado processado pelo Google Analytics. Caso a conexão ocorra através do Facebook, ou seja, caso o usuário crie um login através do Facebook, informações públicas do perfil também são coletadas. Caso o usuário afirme um aceite (opt-in) através de clique em notificação no próprio site, são coletados os dados de nome, e-mail, e informações de Cookie⁴⁷.

42 SOCIAL MINER. (2018). “O comportamento do consumidor Online em 2018”. Disponível em: https://conteudo.socialminer.com/relatorio-comportamento-do-consumidor?utm_source=ECBR&utm_medium=artigo&utm_campaign=relatorio-comportamento-do-consumidor-2018

43 SOCIAL MINER. Política de Privacidade. Disponível em: <https://socialminer.com/privacidade.html>

44 IDEM.

45 IDEM.

46 SOCIAL MINER. Política de Privacidade. Disponível em: <https://socialminer.com/privacidade.html>

47 IDEM.

Já em relação ao funcionamento da plataforma e coleta de dados de usuários que navegam nos sites dos clientes da Social Miner, os dados coletados são os mesmos mencionados acima quando há opt-in dos usuários. A ferramenta é fortemente amparada na coleta e análise de cookies. Por isso, possui um documento separada com a “política de cookies”⁴⁸ da empresa.

Tal política afirma que a Social Miner coleta cookies “persistentes”, ou seja, “todos aqueles que independentemente da navegação, sempre se mantêm registrados no servidor da Social Miner” e de “sessão”, ou seja, os “comportamentos navegacionais dentro de uma janela única de navegação do usuário”⁴⁹. Cookies de sessão, para fins da empresa, subdividem-se em:

cookies de análise, que possibilitam o reconhecimento e contagem do número de visitantes;

cookies de reconhecimento, que visam reconhecer o retorno dos usuários ao website ou tecnologia;

cookies de rastreamento, que tem como função o registro da visita ao website ou tecnologia, quais páginas foram frequentadas e demais informações de navegação.

Além disso, a política de privacidade⁵⁰ afirma que:

“Quando alguém se torna um cliente da Social Miner, nós usamos plugins de conexão, em especial o Facebook Login, para criar uma base de usuários para a marca do cliente. Os avisos e telas de conexão poderão aparecer ao final da navegação de cada usuário ou ao início, quando o mesmo demonstrar intenção de sair do site do cliente, de forma a não prejudicar a navegação ou atrapalhar eventuais procedimentos de compra”.

48 SOCIAL MINER. Política de Cookie. Disponível em: <https://socialminer.com/cookies.html>

49 IDEM.

50 SOCIAL MINER. Política de Privacidade. Disponível em: <https://socialminer.com/privacidade.html>

Já sobre a Magazine Luíza, o documento relativo à política de privacidade da empresa⁵¹ começa esclarecendo algumas definições iniciais, para os efeitos do documento em referência:

“Cookies: arquivos enviados pelo servidor do site para o computador do Usuário, com a finalidade de identificar o computador e obter dados de acesso, como páginas navegadas ou links clicados, permitindo, desta forma, personalizar a utilização do site, de acordo com o seu perfil;

IP: abreviatura de Internet Protocol. É um conjunto de números que identifica o computador do Usuário na Internet;

Logs: registros de atividades do Usuário efetuadas no site;

Session ID: identificação da sessão do Usuário no processo de inscrição ou quando utilizado de alguma forma o site.

Usuário: todo aquele que passar a usar o site.”

Tanto o e-commerce do Magazine Luiza quanto o aplicativo possuem a mesma política de privacidade elaborada em 23 de Julho de 2015. O documento dispõe que a coleta de dados será realizada a partir do momento em que o usuário “(a) passar a utilizar o site; (b) Interagir com as diversas ferramentas existentes no site, fornecendo as informações voluntariamente; ou (c) entrar em contato através dos canais de comunicação disponíveis no site⁵².” No ato de registro do site e aplicativo, o usuário, além de ter a idade mínima de 18 anos, deve fornecer os seguintes dados: nome completo, apelido, CPF, RG, endereço completo, telefone fixo, data de nascimento, e-mail.

No entanto, a hotpage do aplicativo na google store esclarece que o aplicativo pode coletar dados como Localização aproximada do usuário (via rede) e localização precisa do usuário (via acesso ao GPS). Ademais, o aplicativo pede autorizações para realizar chamadas diretamente, acessar dados do SD card dos celulares dos usuários e pontos como - utilização dos dados para Installer API, acesso direto à Internet, ler serviços de configuração do Google, receber dados da Internet, e acesso a conexões de rede e wi-fi.

Além dos dados dispostos acima, a política de privacidade da empresa dispõe que poderá coletar dados referentes à ati-

51 MAGAZINE LUIZA. (2015). Política de Privacidade. Disponível em: <https://www.magazineluiza.com.br/politica/>

52 IDEM.

vidade dos usuários no site, por meio de logs. Os logs em questão incluem endereço de IP do usuário, ações efetuadas no site - páginas acessadas, data e hora de acesso às funcionalidades do site e quais - e session ID do usuário.

2. Tratamento e Finalidades

O Aviso de Privacidade da Amazon declara que a “informação que coletam de seus clientes ajuda a personalizar e melhorar seus produtos”, e o documento sobre “Anúncios baseados no interesse” (Interest-Based Ads) fala de anúncios direcionados. De acordo com o “Privacy Notice” as informações são compartilhadas com “negócios afiliados que a Amazon não controla”; com “terceiros provedores de serviço” que realizam funções subsidiárias ao negócio da Amazon, em nome da empresa; para enviar ofertas para grupos específicos, nesse caso, é possível opt-out; em caso de compra e venda de novas subsidiárias ou unidades de negócios; em caso de proteção da amazon.com e outros, por razão de suspeita de fraude ou outra ilicitude. Por fim, depois de listar essas hipóteses de tratamento e finalidades de compartilhamento, o documento ressalta que em outras hipóteses em que nossos dados podem ser transferidos para terceiros, seus consumidores são notificados para expressar ou não consentimento.

Na Central de Privacidade da Vivo, temos acesso ao Termo de Tratamento de Dados Pessoais⁵³, de maneira distinta do listada na Central de Privacidade, o Termo não elenca fontes de dados, mas tem uma seção específica sobre tratamento de dados pessoais. Contudo, esta parte do documento não elenca as formas de tratamento, apenas dispõe que a contratada, no caso, a Telefônica, tem a obrigação de tratar os dados pessoais na medida do necessário para a prestação de serviço, sendo vedado tratamento para outras finalidades, a não ser que haja autorização expressa. E, em seguida, dispõe sobre outras obrigações, como a de transparência, para tratar dados de seus clientes.

Já a Central de Privacidade exemplifica as razões para coleta de informações dos clientes:

“a) transações de recargas e uso de crédito; b) melhorar desempenho da rede e corrigir falhas; c) personalizar processos de elaboração de planos; d) avaliar demanda por região; e) ajudar na tomada de decisões estratégicas da Vivo, como a redistribuição do sinal ou remanejamento de carteira de serviço; f) e para marketing direto.”

53 TELEFÔNICA, Termo de Tratamento de Dados Pessoais, julho, 01, 2019 https://www.vivo.com.br/portalweb/ShowPropertyServlet?nodeId=/UCMRepository/CONTRIB_269712

Cabe notar, portanto, que informações sobre um mesmo assunto, o tratamento de dados, encontram-se dispersas e apresentadas de maneira distinta em diferentes documentos ou locais de informação. Bem como também não fica muito claro nos itens c e f se os dados pessoais estão sendo utilizados para formação de perfis que terão acesso a diferenças de planos.

Já o Ifood afirma em sua política de privacidade que os dados coletados são usados para ajudar a empresa a melhorar seus produtos e desenvolver novos, bem como para promover auditorias, análises estatísticas sobre o uso dos serviços, incluindo tendências de consumo e “serviços e comunicações com os clientes”, sem detalhes sobre o que configurariam tais serviços. A empresa ainda deixa claro em sua política que usará os dados de feedback das compras, ou seja, a nota dada por cada usuário a cada compra no aplicativo para “publicar e utilizar tais comentários e feedbacks no website ou aplicativo e em quaisquer materiais de marketing ou publicidade, bem como a analisar, processar e tratar esse feedback de forma isolada ou agregada”⁵⁴. Para tanto, o aplicativo identifica o cliente e seu feedback “através de seu nome de cadastro, foto do perfil do iFood (caso haja uma) e da sua cidade de residência”⁵⁵.

Além disso, dispõe que os dados também são usados para “analisar e solucionar problemas técnicos, bem como identificar e coibir fraudes na utilização do (...) Serviço”⁵⁶ e para o envio de notificações e comunicados importantes, como alterações nas políticas, alterações em prazos, comunicados esses que não podem ser desativados pelo cliente por serem considerados inerentes ao serviço. Uma seção específica da política de privacidade atesta a possibilidade de uso dos dados para fins de marketing digital (direcionado em redes sociais e notificações push) e não-digital (como rádio, panfletos, outdoors).

Outra seção é dedicada à explicação de coleta de cookies e afins. Segundo a seção, “o iFood se utiliza de tecnologias como cookies, pixel tags, armazenamento local ou outros identificadores, tanto de dispositivos móveis ou não, ou tecnologias semelhantes (“cookies e outras tecnologias”), para uma variedade de funções”, como por exemplo para “autenticar a sua conta, promover e aperfeiçoar os serviços do iFood, personalizar a sua experiência e avaliar a eficácia da nossa comunicação e publicidade”⁵⁷. Tais informações, para o Ifood, são consideradas não-pessoais sempre que não combinada com uma informação pessoal.

A política da empresa ainda oferece ao cliente exemplos do uso de tais dados:

54 IFOOD. (2018). Política de Privacidade. Disponível em: <https://www.ifood.com.br/privacidade>

55 IDEM.

56 IDEM.

57 IFOOD. (2018). Política de Privacidade. Disponível em: <https://www.ifood.com.br/privacidade>

“saber o seu primeiro nome nos permite dar boas-vindas a você na próxima vez em que você acessar o iFood. Conhecer seu país e idioma nos permite viabilizar a você uma experiência de compras personalizada e mais útil. Saber que você adquiriu determinado produto ou usou um determinado serviço permite fazer com que sua publicidade e comunicações de e-mail sejam mais relevantes para os seus interesses”⁵⁸.

Em relação a terceiros, o Ifood afirma que poderá compartilhar dados com parceiros com a finalidade de desenvolver campanhas de marketing mais assertivas e que “somente compartilhará dados com parceiros que possuem política de privacidade que ofereça níveis compatíveis de proteção àquele oferecido”⁵⁹ pela sua política. Ademais, terceiros que realizem marketing dentro do aplicativo ou site do Ifood, ou seja, que promovam propaganda de produtos terceiros em tais espaços, “podem utilizar cookies e outras tecnologias próprios nos serviços do iFood, tais como: Facebook, Google Analytics e Double Click”⁶⁰ para aferir o andamento das campanhas de marketing.

A política de privacidade afirma que Integrantes do grupo Ifood também poderão ter acesso a alguns dos dados dos clientes, bem como empresas de processamento de pagamentos, empresas parceiras contratadas pelo Ifood para prestar serviços como marketing e análise de dados, restaurantes associados que fazem os pedidos entregues, serviços de redes sociais (quando o cliente compartilhe diretamente em seu Facebook uma compra recente, por exemplo) e, no caso de informações como nome e foto de perfil, com outros usuários do aplicativo.

A empresa também afirma que o armazenamento dos dados se dá “em serviços de nuvem confiáveis de parceiros que podem estar localizados no Brasil ou em outros países que ofereçam serviço de armazenamento de nuvem confiáveis e usualmente utilizados por empresas de tecnologia”⁶¹ e retidos pelo tempo determinado pela legislação aplicável, em termos amplos.

A empresa ainda se propõe a cumprir a legislação acerca da transferência de dados para autoridades judiciais, mas vai além, afirmando que “o iFood se reserva o direito de compartilhar informações sobre seus usuários a terceiros quando houver motivos suficientes para considerar que a atividade de um usuário é suspeita, ilegal ou prejudicial ao iFood ou a

58 IDEM.

59 IDEM.

60 IDEM.

61 IFOOD. (2018). Política de Privacidade. Disponível em: <https://www.ifood.com.br/privacidade>

terceiros”.⁶²

Em relação à segurança, o Ifood afirma seguir “privacy by design”. A empresa não detalha o que seria tal indicativo, mas afirma na mesma seção que: “Só tratamos os seus dados mediante alto grau de segurança”.

Por sua vez, a política de privacidade da Social Miner define, já em sua abertura, que ao usuário:

*“que não concorda com o conteúdo desta política, não é recomendável baixar nossos materiais em utilizar quaisquer de nossos serviços e, caso tenha baixado ou utilizado e queira exercer seus direitos de restrição, retificação, exclusão ou oposição, entre em contato pelo privacy@socialminer.com”.*⁶³

Sobre o uso dos dados, a empresa afirma que os dados coletados serão usados pela equipe de marketing para contato pró-ativo da equipe de vendas. Ademais, a empresa afirma que poderá cruzar dados coletados através do login do Facebook com dados de navegação, “de forma a permitir uma maior personalização das mensagens enviadas pela nossa empresa” aos clientes.⁶⁴

Os dados coletados de usuários em sites dos clientes da Social Miners servem, ainda, para “uma maior personalização das mensagens enviadas pela empresa (contratante), bem como a análise do comportamento de compra feita automaticamente pelos algoritmos de inteligência artificial” da empresa.⁶⁵ Ou seja, é o cruzamento dos dados coletados, sobretudo os cookies de navegação, que viabilizam a personalização da propaganda recebida pelos usuários que acessam sites de empresas que contrataram os serviços da Social Miner.

Assim, os dados pessoais coletados dos usuários são usados e processados de forma automatizada pelos algoritmos para entender padrões de comportamento e criar audiências segmentadas para as campanhas feitas pela plataforma. Conforme política de privacidade, a empresa utiliza “automatização no processamento de dados para analisar as movimentações do usuário ou visitantes dentro do website, identificando conteúdos e produtos de interesse e, com base nisso, sugerir produtos de forma personalizada às preferências individuais”.⁶⁶

62 IDEM.

63 IDEM.

64 SOCIAL MINER. Política de Privacidade. Disponível em: <https://socialminer.com/privacidade.html>

65 IDEM.

66 IDEM.

Segundo a política, os dados “gerais de cadastro e clique serão usados para otimizar as campanhas feitas através da nossa plataforma e estarão sempre à disposição (dos contratantes), podendo ser extraídos a qualquer momento, bem como integrados ao software de CRM (dos contratantes)”⁶⁷. CRM é a sigla para “Customer Relationship Management”, ferramenta que facilita o cadastro e registro de informações de cada cliente. Os usuários do site do contratante, conforme documento, possuem direito de se descadastrar da base de dados, embora não haja clareza sobre como tal pedido seria feito e como os usuários tomam conhecimento de tal possibilidade.

Além disso, a política de privacidade afirma que os dados coletados pela empresa também “serão usados apenas para eventuais cobranças de serviços, comunicados internos e envio de materiais educativos ou gerar pesquisas de mercado”. Sobre tais pesquisas, a Social Miners define que “os dados usados para estudos gerais de comportamento do consumidor terão as informações pessoais dos usuários deletadas” e que, nesse caso, eles não se configuram mais um dado pessoal, e sim um “mero conjunto de dados anônimos para fins de estudo e pesquisa”⁶⁸.

Sobre a proteção dos dados coletados, a empresa afirma que o acesso aos dados pessoais “é restrito aos funcionários da Social Miner - mais especificamente, às áreas de vendas, financeiro e marketing” e que nenhuma informação pessoal poderá ser divulgada publicamente. Além disso, a empresa afirma que “se compromete a não vender, alugar ou repassar suas informações para terceiros” a não ser que exigida judicialmente.⁶⁹

O acesso aos dados dos usuários pelo contratante se dá com base no comportamento dos usuários e individualização de campanhas sem que o contratante consiga acessar o comportamento individualizado de um usuário diretamente na plataforma da Social Miners. Ademais, a empresa afirma ser terminantemente contra a “cookiepool”, prática de compartilhamento de bases de dados sobre cookies entre seus clientes, ou seja, entre os sites das empresas contratantes.

Por fim, destaca-se que a política afirma que, “Caso você seja um usuário visitante de um cliente da Social Miner, recomendamos que entre em contato diretamente com o cliente, exercendo seus direitos de privacidade”⁷⁰. Também afirma que não coleta dados de menores de 13 anos. Sobre o período de armazenamento, a empresa afirma que mantém os dados enquanto necessário para o provimento dos serviços, enquanto possuem consentimento para tal ou enquanto determinado pela lei, apagando certos dados com inatividade contínua após 5 anos.

67 IDEM.

68 SOCIAL MINER. Política de Privacidade. Disponível em: <https://socialminer.com/privacidade.html>

69 IDEM.

70 IDEM.

Em relação ao Magazine Luiza, a política de privacidade da empresa esclarece que os dados e informações coletadas serão adicionados ao banco de dados do site do Magazine Luiza, de titularidade e propriedade da empresa. Os dados em questão serão armazenados em ambiente seguro ao qual só terão acesso pessoas qualificadas e autorizadas pela empresa. No entanto, a empresa se exime de eventuais danos e prejuízos ocasionados por falhas, vírus ou invasões do banco de dados do site, salvo nos casos de dolo ou culpa da empresa.

A empresa também esclarece que os dados dos usuários não serão compartilhados, vendidos ou apresentados à terceiros. Adicionalmente, dispõe que o usuário do site é titular dos dados e está apto a adicionar, excluir ou modificar qualquer informação ligada ao seu perfil.

Ainda no que tange o tratamento dos dados, a política de privacidade esclarece que os dados pessoais coletados poderão ser utilizados para as seguintes finalidades:

“(1) Efetuar qualquer comunicação resultante de atividade do próprio site ou a identificação do respectivo destinatário; (2) Responder a eventuais dúvidas e solicitações do Usuário; (3) Fornecer acesso à área restrita do site ou suas funcionalidades exclusivas; (4) Cumprimento de ordem legal ou judicial; (5) Constituir, defender ou exercer regularmente direitos em âmbito judicial ou administrativo; (6) Elaborar estatísticas gerais, para identificação do perfil dos Usuários e desenvolvimento de campanhas do Magazine Luiza; (7) Garantir a segurança dos Usuários; (8) Manter atualizados os cadastros dos Usuários para fins de contato autorizado a ser feito por telefone, correio eletrônico, SMS, mala-direta ou por outros meios de comunicação; (9) Informar a respeito de novidades, promoções e eventos do Magazine Luiza e seus parceiros comerciais”⁷¹.

A empresa ainda se reserva o direito de enviar emails diários com ofertas aos clientes cadastrados, que poderão ser cancelados por meio de descadastramento via link presente em todos os emails promocionais.

Por fim, no referente à cookies, o MagaLu deixa claro que pode fazer a utilização do primeiro, cabendo ao usuário desabilitá-los em seu navegador de preferência. No tangente à dados de registro de atividades, a empresa reserva o seu uso para a verificação de casos de investigação de fraudes ou de alterações indevidas em seus sistemas e cadastros.

71 IDEM.

3. Relação com as empresas GAFAM

Quanto à Amazon Prime Video, observamos uma relação direta com a empresa Brasileira Vivo, afetando o entendimento ou qualquer tentativa de fácil compreensão sobre onde começa e onde termina a relação dessas duas empresas com nossos dados. A multiplicidade de documentos que tratam do tema, nas duas plataformas, torna inviável uma compreensão informada, seja do consumidor comum, seja de consumidores que tenham mais afinidade com o debate de proteção de dados.

Considerando a conexão do iFood com as GAFAM, percebemos três tipos de relacionamento. Em primeiro lugar, a empresa permite que os usuários acessem suas contas através de seus perfis no Facebook. A outra opção é realizando um novo cadastro com o email pessoal, mas é menos destacada no aplicativo. Em segundo, ao menos a política de privacidade atesta a possibilidade de existência de botões de redes sociais, em que os usuários poderiam compartilhar diretamente em seu Facebook detalhes sobre seus pedidos. Em terceiro, o iFood usa o Google Analytics, coletando informações sobre o comportamento dos usuários no site para mapear tendências.

Dessa forma, o iFood tanto disponibiliza informações para as GAFAM, quanto coleta dados delas. Por exemplo, sobre o Facebook, a política de privacidade afirma que:

“ao utilizar o Facebook para se inscrever no nosso serviço, você estará permitindo que o iFood acesse as informações pessoais em sua conta do Facebook, tais como seu nome, e-mail, gênero, idade e telefone (caso o tenha cadastrado no Facebook). As informações que poderemos obter, nesse caso, dependem das suas configurações de privacidade junto ao serviço de rede social”.⁷²

Considerando a relação do aplicativo com o iFood, houve caso em 2018 de um boato que circulou nas redes e afetou alguns perfis do Facebook. Alguns usuários mudaram o sobrenome no Facebook para “iFood” para ganhar um cupom de desconto no aplicativo. No entanto, tal cupom era uma mentira, e os usuários que fizeram a alteração, devido a políticas da própria plataforma, foram obrigados a manter o nome trocado por pelo menos 60 dias⁷³.

Já houve, também, iniciativa do iFood de criação de um bot que interagiu com usuários através do Facebook Messenger

72 IDEM.

73 LETIERI, R. (2019). Usuários colocam iFood no sobrenome e não conseguem mudar. Techtudo. Disponível em: <https://www.techtudo.com.br/noticias/2019/05/usuarios-colocam-ifood-como-sobrenome-no-facebook-e-nao-conseguem-mudar.ghml>

para que os usuários pudessem efetuar pedidos diretamente da rede social. Tal funcionalidade não opera mais⁷⁴. Ademais, o Google tem funcionalidade de realizar comprar em aplicativos de donos de celulares de forma mais rápida. Batizado de “Pagar com Google”, esse recurso funciona para compras no iFood e no Magazine Luíza.⁷⁵

No que se refere à relação da Social Miner com empresas que integram o GAFAM, a empresa se reserva o direito de cruzar dados de navegação e login no Facebook para fins de aperfeiçoamento dos produtos oferecidos. A plataforma de direcionamento de conteúdo oferecida pela Social Miner é alimentada por dados de navegação dos usuários, além dos dados de login em plataformas como Facebook

A política de privacidade da empresa menciona que dados de navegação de visitantes ao site e plataforma serão transformados em dados pelo Google Analytics e que, caso o visitante se conectar com a marca via Facebook login, suas informações públicas básicas, como nome, idade, sexo, bem como suas informações demográficas serão coletadas, mediante aprovação prévia, e serão cruzadas com seus dados de navegação, de forma a permitir uma maior personalização das mensagens enviadas pela nossa empresa.

Um outro ponto de relação com o Facebook fica claro quando o mesmo documento menciona a utilização de plugins de conexão, em especial o Facebook Login, para criar uma base de usuários/clientes para a marca contratante. A empresa ainda oferece a possibilidade de mostrar avisos e telas de conexão com a rede social no início da navegação ou quando o consumidor desejar que vai sair do site de uma determinada marca. Ou seja, a eventual coleta de dados pessoais dos usuários realizada pela Social Miners para a criação de bases de dados pode não ser devidamente informada ao consumidor. E, considerando que a atuação da Social Miner é com segmentação de conteúdo para fins de marketing digital, a empresa pode inferir em práticas de profiling dos consumidores.

Sobre MagaLu, a conexão clara do site e aplicativo com as GAFAM é via autenticação com Perfil do Facebook e Conta do Google, no entanto o app esclarece que nenhum conteúdo será postado em nome dos titulares das contas. Além disso, ambas plataformas permitem o compartilhamento de ofertas via Facebook, Twitter, Google Plus, Whatsapp e email pessoal. A política de privacidade não dispõe sobre uso compartilhado de dados com as plataformas ou a utilização de google analytics para analisar comportamentos de compra de seus usuários.

74 LIMA, L. (2017). iFood lança chatbot para pedir pizza no Messenger, mas será se funciona?. Novarejo. Disponível em: <https://portalnovarejo.com.br/2017/07/ifood-chatbot-messenger/>

75 GAZETA DO POVO. (2017). iFood e Magazine Luiza estreiam sistema de pagamentos online do Google no Brasil. Disponível em: <https://www.gazetadopovo.com.br/economia/nova-economia/ifood-e-magazine-luiza-estreiam-sistema-de-pagamentos-online-do-google-no-brasil-24pqs32pbqzn86seh3ktp7i/>

No entanto, a estratégia digital da empresa tem muito envolvimento com o Facebook. Em 2012, o Magalu apresentou a ideia de habilitar lojas na plataforma Facebook e constituir uma rede de F-Commerce onde os usuários poderiam constituir suas próprias lojas que seriam afiliadas ao Magazine Luiza⁷⁶.

Um outro programa interno da empresa chamado Magazine Você tinha como objetivo remunerar usuários com pequenas comissões por recomendar determinados produtos em redes sociais. De acordo com o website tecnoblog⁷⁷, o programa funcionava da seguinte maneira:

Tendo uma conta no Facebook, os usuários da rede social já podem usar o aplicativo Magazine Você para recomendar produtos ofertados pela Magazine Luiza para seus amigos no serviço. A lógica de funcionamento é semelhante à de qualquer programa de afiliados: há uma comissão por item vendido, referente a um percentual calculado sobre o valor da venda.

Esse percentual depende da categoria do produto que está à venda. Por exemplo, itens de informática garantem à pessoa que recomendou o produto por meio do Magazine Você 2,5% do valor pago pelo produto.

No site da empresa não é mais possível encontrar informações sobre o Magazine Você e a página do programa no Facebook se encontra indisponível.

4. Casos de violações de privacidade relacionados à marca

Em 2019, o iFood enviou para uma série de clientes promoção em que o usuário ganharia um suco de graça após responder a um questionário⁷⁸. O link para o questionário, no entanto, possuía um erro de digitação. Usuários que entraram no link errado foram encaminhados para uma página que recomendava o download de um antivírus que, na verdade, infectou os dispositivos dos clientes. Houve, ainda, caso em que uma página falsa do iFood levava usuários a digitar login e senha para acessar o serviço de delivery. No entanto, ao fazer o login, houve o roubo das credenciais do usuário.

Ademais, em agosto de 2018, a vendedora virtual criada pelo Magazine Luiza, Lu, foi vítima assédio online de alguns segui-

76 JESUS, A. (2012). Magazine Luiza lança F-commerce no Facebook e Orkut. Techtudo. Disponível em: <https://www.techtudo.com.br/noticias/noticia/2012/02/magazine-luiza-faz-sucesso-com-seu-f-commerce-no-facebook-e-orkut.html>

77 VELOSO, T. (2012). Magazine Luiza lança programa de comissão para Facebook. Tecnoblog. Disponível em: <https://tecnoblog.net/74606/magazine-luiza-facebook/>

78 OLIVEIRA, F. (2019). Hackers aproveitam erro de digitação em campanha do iFood para infectar consumidores com vírus. Folha de São Paulo. Disponível em: <https://www1.folha.uol.com.br/mercado/2019/03/hackers-aproveitam-erro-de-digitacao-em-campanha-do-ifood-para-infectar-consumidores-com-virus.shtml>

dores das plataformas da Loja e o caso foi repercutido pelo portal BuzzFeed⁷⁹. Na ocasião, um gif da avatar acompanhado de uma mensagem de repressão às cantadas desrespeitosas recebidas foi postado nas redes sociais do Magazine Luiza e ajudaram a chamar a atenção para o debate a respeito de assédio sexual online no Brasil.

Outro caso que vale mencionar é a criação de páginas falsas da empresa no Facebook com o intuito de roubar dados pessoais, inclusive informações bancárias, dos clientes da empresa. Em 11 de fevereiro de 2019, o DFNDR LAB⁸⁰ postou em uma rede social a respeito da criação de páginas falsas no Facebook com os clientes do Magazine Luiza como alvo, até o momento as páginas somavam mais de 1000 usuários.

79 ORRICO, A. (2018). Tem uma galera dando em cima da vendedora virtual da Magazine Luiza. BuzzFeed. Disponível em: <https://www.buzzfeed.com/br/alexandreorrico/vendedora-virtual-da-magazine-luiza>

80 SOUSA, G. (2019). Páginas Falsas da Magalu no Facebook Tentam Roubar Dados. Adnews. Disponível em: <https://adnews.com.br/internet/paginas-falsas-da-magalu-no-facebook-tentam-roubar-dados/>

III. AVALIAÇÃO DO REGIME JURÍDICO DE PROTEÇÃO DE DADOS PESSOAIS PARA ABORDAR AS DINÂMICAS DAS EMPRESAS ANALISADAS

1. Regime jurídico de proteção de dados no Brasil

Desde 2018, o Brasil conta com uma Lei Geral de Proteção de Dados Pessoais (Lei 13709/2018), matéria fruto de intensas discussões entre os stakeholders do país e arranjos políticos. Mesmo antes da sua aprovação, no entanto, o Brasil já contava com legislações prévias que salvagam, em alguma medida, direitos à privacidade. A Constituição Federal, o Código de Defesa do Consumidor (Lei 8078/90), a Lei do Habeas Data (Lei 9507/97) e o Marco Civil da Internet (Lei 12965/2014) e o Decreto que o regulamenta (Decreto 8.771/16) já delimitavam princípios e diretrizes para a proteção da privacidade⁸¹. Além disso, várias regulações setoriais⁸² também tratam, ainda que tangencialmente, da proteção de dados pessoais, principalmente no sistema financeiro e de saúde. Contudo, até a aprovação da LGDP, o Marco Civil da Internet, lei sancionada em 2014, foi a primeira legislação a tratar especificamente da proteção de dados na Internet.

Depois de uma série de consultas multisetoriais, o Marco Civil da Internet tornou-se uma legislação conhecida e reconhecida internacionalmente e serve, entre outras coisas, como uma carta de direitos e deveres na Internet no Brasil. Também foi a fonte mais direta de direcionamento para o que viria a se consolidar na LGDP em relação à proteção de dados pessoais, fundamentação do direito à privacidade e introdução da noção de consentimento em acordos na Internet.

Tal lei, por exemplo, apresentou disposições iniciais importantes sobre a guarda e compartilhamento dos dados dos usuários. Os artigos 10 e 11 já afirmam positivamente a importância do cuidado na coleta, tratamento e transmissão dos dados dos usuários da Internet. Por exemplo, dispõem que os provedores de Internet só disponibilizarão registros de conexão e de acesso de aplicações da Internet mediante ordem judicial. Especificamente, o artigo 11 afirma que:

“Em qualquer operação de coleta, armazenamento, guarda e tratamento de re-

81 PRIVACY INTERNATIONAL. (2019). State of Privacy Brazil. Disponível em: <https://privacyinternational.org/state-privacy/42/state-privacy-brazil>

82 MONTEIRO, R. L. (2017). “Proteção de dados e a legislação vigente no Brasil”. Baptista Luz. Disponível em: <http://baptistaluz.com.br/wp-content/uploads/2017/11/Privacy-Hub-Leis-Setoriais.pdf>

gistros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros”.

De forma ainda mais clara, a lei defende “a inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação” durante o uso da Internet (artigo 7). Notadamente, o Marco Civil também lançou as bases para o que a LGDP consolidaria como, salvo exceções expressas, umas das medidas necessárias para a coleta de dados: o consentimento dos usuários. Diz o texto, em seu artigo 16, que:

*“Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:
I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente (...); II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular”.*

Por tratar apenas de Internet, o Marco Civil não solucionou todas as áreas cinza em relação à proteção de dados no país, ainda assim, já apontava para alguns princípios e responsabilidades. À propósito, mesmo antes da aprovação do Marco Civil, outras legislações já eram usadas para fazer valer questões relativas à proteção de dados e já estavam sendo construídas para acompanhar o que viria a ser a LGDP. Por exemplo, o Código do Consumidor (CDC), datado de 1990, em seu artigo 43, dispõe que:

“O consumidor (...) terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos”.

Também afirma que o consumidor poderá exigir a correção de dados que se encontrem inexatos. Mesmo que projetada em um período em que a Internet comercial ainda não expunha os desafios relativos à privacidade de hoje em dia, o CDC já provinha insumo que poderia ser usado, ainda que de forma tangencial, para proteger o usuário.

Algumas resoluções (atos administrativos normativos que provém de outras autoridades que não o Poder Executivo) mais recentes também trataram do tema. Por exemplo, em 2018, alguns meses antes da sanção da LGDP, o Banco Central publi-

cou a resolução 4.658 de abril de 2018, dispondo sobre a política cibernética e a contratação de serviços de armazenamento e processamento de dados em instituições financeiras do Brasil.

A LGDP, por sua vez, começou a ser debatida ainda em 2010, quando o Ministério da Justiça promoveu uma consulta pública sobre o tema, e culminou no envio, por parte do Governo Federal de um projeto de lei para o Congresso Nacional. Na casa legislativa, o projeto foi apensado, ou seja, anexado a outras proposições que já estavam em debate, e foi discutido em Comissões Especiais especificamente designadas para abordar o tema. Após dois anos de debates intensos, repletos de audiências públicas e consultas, a matéria foi aprovada e sancionada, dando início a um período de adaptação que perdura até o momento de elaboração do artigo.

A lei veio solucionar eventuais conflitos entre as normas já existentes e adequar o Brasil à tendência internacional de se estabelecer uma lei geral de proteção dos dados pessoais. Por exemplo, a LGDP, abriu as portas para o Brasil ser considerado a ocupar a lista de países que estão de acordo com disposições presentes na General Data Protection Regulation (GDPR). Tal regulação, da União Europeia, alcançou aplicação extraterritorial ao impor medidas de proteção à privacidade similares a qualquer país que pudesse, direta ou indiretamente, estar conectado com o tratamento de dados pessoais de europeus.

Cumprir adicionar que, no final de 2019, o Governo Brasileiro editou os decretos n. 10.046 e 10.047/2019, que dispõem sobre o exame de governança e o compartilhamento de dados pessoais no âmbito da Administração Pública Federal e dos Institutos de Registro de Base de Cidadania e do Comitê Central de Governança Dados. Apesar da proposta inicial dos decretos ter por objetivo uma maior harmonia entre as atividades de processamento e coleta de dados pessoais do governo, o texto promove confusão e traz novas definições para alguns dos conceitos tratados na Lei Geral de Proteção de Dados Pessoais. Ambos decretos são objeto de discussões no Congresso Nacional Brasileiro que propõem a sua revogação e suspensão imediata dos seus efeitos.

2. Pontos principais da Lei de Proteção de Dados no que diz respeito às práticas das quatro empresas selecionadas

A seguir, considerando as práticas apresentadas nas políticas de privacidade e termos de serviço das 4 empresas com modelos de negócio baseados em dados que selecionamos para este estudo, elencamos partes da lei que dizem respeito a essas práticas, visando analisar tanto se elas são compatíveis com a lei que entrará em vigor em agosto de 2020 e se o marco legal atual é capaz de lidar com todas as previsões de coleta, tratamento, compartilhamento e armazenamento que

fazem parte do modelo de negócios dessas empresas.

A) FINALIDADE, CONSENTIMENTO E COMPARTILHAMENTO COM TERCEIROS

De forma específica, a LGDP definiu dado pessoal como uma informação relacionada a pessoa natural identificada ou identificável. Em, em seu artigo sexto, listou uma série de princípios que devem guiar o tratamento de tais dados no país. São eles, conforme o artigo 6, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

Além desses princípios, a lei dispõe que o consentimento é requisito para o tratamento de dados pessoais pelo setor privado, a não ser no caso de cumprimento de obrigação legal e outras exceções pontuais, como casos de legítimo interesse do controlador. Nesse caso específico, a lei dispõe que “quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados” (artigo 10, parágrafo 1). Ou seja, é vedado a quem for tratar dados dos titulares o uso de tais informações para fins que extrapolam o objetivo inicial da relação entre as partes. A lei também dispõe no parágrafo 5º do artigo 7 que o controlador que obtiver consentimento e precisar comunicar ou compartilhar dados com outros controladores deverá obter consentimento específico para esses fins (também ressalvadas as hipóteses de dispensa de consentimento).

A lei também dispõe que o consentimento deve ser destacado das demais cláusulas contratuais e deve referir-se a finalidades determinadas, podendo ser revogado a qualquer momento. Sendo que o titular também tem direito a acesso facilitado às informações sobre o tratamento de seus dados, constando:

finalidade específica do tratamento;

forma e duração do tratamento, observados os segredos comercial e industrial;

identificação do controlador;

informações de contato do controlador;

informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

responsabilidades dos agentes que realizarão o tratamento; e

direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

Considerando as práticas das empresas analisadas a luz do que diz a LGDP à respeito do consentimento, do compartilhamento de dados com terceiros e dos princípios, algumas questões merecem atenção.

Em relação à Social Miner, por exemplo, não há clareza em relação à forma como se dá o consentimento do usuário para que seus dados passem a integrar a base de dados da empresa. O consentimento para a coleta dos dados de navegação, amparados na coleta de cookies, ocorre com um aceite dos usuários nos sites de cada cliente da Social Miner a partir de notificações nos cantos superiores ou inferiores da tela. No entanto, não se sabe se há um padrão de texto informado aos usuários nos sites de cada cliente ou se as notificações de rastreamento de cookies são específicas o suficiente para que o usuário compreenda que a coleta será usada não apenas para a melhora da navegação, mas também com fins claros de marketing digital.

A política de privacidade ainda afirma que os avisos de coleta de dados “poderão aparecer ao final da navegação de cada usuário ou ao início, quando o mesmo demonstrar intenção de sair do site do cliente, de forma a não prejudicar a navegação ou atrapalhar eventuais procedimentos de compra”⁸³. Acreditamos que os usuários deveriam ser informados da possibilidade de coleta de seus dados sempre e logo ao início da navegação, de forma a alcançar maior e mais rápido entendimento do usuário sobre a coleta.

Além disso, a empresa apresenta fortes disposições em relação ao compartilhamento de dados com terceiros. Segundo a política de privacidade, “além da própria Social Miner, nenhuma outra empresa ou cliente terá acesso aos dados e informações pessoais dos seus leads. Somos contra a política de Cookiepool e jamais compartilharemos base entre os nossos clientes”⁸⁴. Tal disposição é boa considerando a privacidade dos usuários, mas pode ter sido inserida na política de privacidade considerando a própria pressão do mercado de marketing amparado em cookies que rechaça a noção de cookiepool.

As demais empresas analisadas também apresentam pontos críticos no que diz respeito ao consentimento e compartilhamento com terceiros. No caso da Amazon Prime Video contratada pela a manutenção desses direitos é ainda mais complexa. A começar pela dificuldade de se encontrar as políticas de privacidade que regem esse serviço, se contratado via operadora de telefonia. Conforme o contrato com a Vivo, o serviço é regido por termos de uso de ambas as empresas. Mas os termos de uso para assinatura do Prime Video pelos clientes Vivo nada dispõe sobre proteção de dados daqueles que contrataram esse serviço, pois tratam apenas de formas de contratação, pagamento e cancelamento. O Centro de Privaci-

83 SOCIAL MINER. Política de Privacidade. Disponível em: <https://socialminer.com/privacidade.html>

84 IDEM.

dade da Vivo⁸⁵, página que fornece informações sobre privacidade e segurança que dizem respeito ao plano de celular ou banda larga oferecidos pela operadora não é referenciada no termo de assinatura do Amazon Prime Video pela Vivo.

Nos termos de uso da Amazon Prime Video, que é hiperlinkado no contrato com a Vivo, os clientes também encontram link para o Aviso de Privacidade (Privacy Notice) e a política de anúncios de Amazon, mas todos eles estão em inglês, ou seja, apenas com insistência de pesquisador os consumidores chegariam às políticas de privacidade da Vivo e da Amazon e, no caso da Amazon, teriam que saber inglês para entendê-la, mesmo que o serviço seja oferecido no Brasil e em parceria por empresa aqui estabelecida. Essas circunstâncias não apenas impossibilitam um consentimento informado, como também dificultam qualquer acesso à informação ou controle do uso de dados por parte dos consumidores.

Além dessa dificuldade de entender quais políticas de privacidade se aplicam, quais as empresas controladoras e de que tipos de dados estamos tratando, tanto a política de privacidade da Vivo como o Aviso de Privacidade da Amazon abrem margem para mais atores terem acesso aos dados de seus consumidores. Ora, se o consentimento já era dificilmente informado no que tange o tratamento de dados por essas empresas, a situação piora ainda mais quando falamos de compartilhamento com terceiros.

O Aviso de Privacidade da Amazon⁸⁶, ao responder à pergunta “A Amazon compartilha informações que recebe?”, anuncia que a “empresa não vende informações de seus clientes”, mas elenca atores com quem compartilha esses dados. Entre eles estão o que o Aviso de Privacidade denomina “affiliated business we do not control” (ou seja, negócios filiados dos quais não temos controle), não fica especificado quem seriam esses afiliados, o texto apenas remete a outro texto onde temos alguns exemplos de marcas, principalmente, norte-americanas, como Starbucks, OfficeMax, Verizon Wireless, Sprint, T-Mobile, AT&T, J&R Electronics, Eddie Bauer and Northern Tool + Equipment. Mas pode-se aferir que a Vivo também entraria nessa categoria. Por fim, também afirma que em caso de compra ou venda dos negócios da Amazon, “informações de consumidores são considerados ativos do negócio a serem transmitidas”, ainda que afirme que políticas de privacidade prévias à venda continuariam. Todas essas previsões abrem brechas enormes para se questionar o respeito ao princípio da finalidade e o consentimento do consumidor acerca do uso de seus dados.

Já o iFood diz que “integrantes do grupo food” e “provedores de serviços e outros parceiros” podem ter acesso a dados de clientes⁸⁷. A política é ampla e não deixa claro quais dados poderiam ser compartilhados, dando a entender, inclusive, que

85 VIVO. Centro de privacidade. Disponível em: https://www.vivo.com.br/portalweb/appmanager/env/web?_nfls=false&_nfpb=true&_pageLabel=vivoVivoInstPrivacidadePage&WT.ac=portal.amarca.privacidade&#

86 AMAZON. Amazon Privacy Notice. Disponível em: <https://www.amazon.com/gp/help/customer/display.html?nodeId=468496>

87 IFOOD. (2018). Política de Privacidade. Disponível em: <https://www.ifood.com.br/privacidade>

a empresa poderá terceirizar para subsidiárias os serviços do iFood e, conseqüentemente, sua base de usuários. Também afirma que o compartilhamento de dados com terceiros, para fins de marketing, ocorre apenas quando tal terceiro possui padrões de proteção da privacidade similares ao do próprio iFood, mas não detalha exatamente quais tipos de dados poderão ser compartilhados. Com isso, não é possível aferir se tais dados seriam os estritamente necessários para fins de marketing, ou se eles extrapolam tal objetivo. Em todo o caso, a política não é específica o suficiente e parece abrir para um foro muito ampliado a possibilidade de acessos da base de usuários do serviço.

O Magazine Luiza, por sua vez, possui uma política de privacidade relativamente omissa com relação à obtenção de consentimento dos usuários. O documento dispõe apenas sobre a utilização dos dados e uma posterior possibilidade do cliente realizar o descadastramento da base de dados de emails de marketing e não sobre a obtenção de autorização prévia, informada e consentida que oriente o tratamento dos dados. No tangente ao compartilhamento dos dados, a política de privacidade dispõe que “não compartilhará, venderá ou apresentará os dados dos Usuários para terceiros, que não sejam seus parceiros”⁸⁸. Assim como outros casos aqui mencionados, a política do Magazine Luiza segue ampla e não dispõe sobre quem seriam os eventuais parceiros do Magazine Luiza e nem se o compartilhamento seria feito para fins de marketing.

B) USO DE COOKIES

Além de compartilhamento com terceiros, as 4 empresas afirmam utilizar cookies e diferentes tipos de webtrackers. Ao contrário do disposto na Regulação Geral de Proteção Dados (General Data Protection Regulation - GDPR), a legislação brasileira não tem previsões específicas para o uso dessas tecnologias. Contudo, podemos questionar como o uso de cookies e tecnologias semelhantes de rastreamento podem se encaixar nos princípios da finalidade, adequação, necessidade e até mesmo da não discriminação, todos previstos na lei brasileira.

Das empresas analisadas, a Social Miner é a única que possui uma política específica de cookies, algo esperado considerando que os serviços prestados pela start-up são altamente baseados no rastreamento de cookies para fins de campanha de marketing. Tal política explica o que são e quais são os tipos de cookies coletados pela empresa.

A própria política de privacidade da Social Miner cita a GDPR para dispor que a start-up estaria de acordo com o que diz o regulamento europeu. A presença de tal indicativo é louvável. Ainda assim, a política afirma ser responsabilidade do cliente da Social Miner informar os usuários sobre a coleta de cookies e dados pessoais (em caso de conexão via email ou redes sociais), algo compreensível do ponto de vista operacional, mas que deixa o usuário em uma situação de vulnerabilidade

88 MAGAZINE LUIZA. (2015). Política de Privacidade. Disponível em: <https://www.magazineluiza.com.br/politica/>

por depender dos padrões de transparência do cliente (contratante da Social Miner).

Já o iFood chega a determinar que informações sobre as atividades dos usuários no website ou aplicativo da empresa são agregadas e consideradas como dados “não pessoais”, por supostamente não permitirem a identificação de cada usuário. A política também classifica “a idade do indivíduo, preferências individuais, idioma, CEP e código de área” como dados não pessoais⁸⁹. Tais classificações podem indicar uma tentativa de excluir esses tipos de informações das proteções legais, já que dizem respeito a dados que claramente são pessoais e, sem o devido tratamento, podem facilmente ser usados para identificar indivíduos específicos. Assim, a disposição do iFood em tentar classificar certos dados como não pessoais é grave e deixa portas abertas para uma potencial violação da privacidade dos clientes da empresa.

No ponto da coleta dos cookies dos usuários dos serviços estudados, cabe pontuar que estes dados servem como identificadores gerados ou coletados sobre um usuário. Ao adotar o conceito de dado pessoal como “informação relacionada a pessoa natural identificada ou identificável”⁹⁰ pode-se dizer que a LGPD considera o cookie que atua como um identificador eletrônico⁹¹, ou que tenha por objetivo inferir perfis de compra, como uma forma de coletar dado pessoal.

Ademais, a política de privacidade do iFood diz que “em algumas de nossas mensagens de e-mail, (o Ifood usa) uma ‘URL click-through’ (endereço externo) vinculada ao conteúdo do iFood. Quando os clientes clicam em uma dessas URLs, os usuários são enviados para um servidor diferente antes de chegarem à página de destino no nosso serviço. (O Ifood monitora) esses dados de click-through para entender o interesse em determinados tópicos e avaliar a eficácia das comunicações com os nossos clientes”⁹². Caso o cliente não queira ser monitorado de tal forma, a política demanda que ele “não clique em texto ou links contidos em mensagens de e-mail enviadas pelo iFood”⁹³.

Aparentemente, a prática de direcionamento dos usuários para servidores antes da página final de destino não é informada aos clientes em momento algum - salvo àqueles que lerem a política de privacidade em sua completude antes mesmo de clicar em algum link veiculado pelo iFood em seus emails enviados para os clientes. Tal prática não é ideal e pode ferir os direitos dos usuários de consentirem com clareza a respeito da coleta de seus dados.

89 IFOOD. (2018). Política de Privacidade. Disponível em: <https://www.ifood.com.br/privacidade>

90 BRASIL. Lei 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/L13709.htm

91 GOMES, M. C. O. (2018). Cookie notice: informar, obter e por fim coletar dados pessoais. (JOTA). Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/cookie-notice-informar-obter-e-por-fim-coletar-dados-pessoais-23112018>

92 IDEM.

93 IDEM.

No caso do Magazine Luiza, a política de privacidade do aplicativo⁹⁴ apresenta um ponto específico sobre cookies, dispondo que o site/aplicativo poderão fazer o uso destes, cabendo ao usuário desabilitá-los. O documento ainda explicita que recomendações de produtos serão realizadas a partir de um cookie que identifica a navegação do usuário. Neste caso, a navegação engloba o comportamento do usuário dentro do site/aplicativo com foco em fatores como a) se houve navegação ou compra; b) itens visualizados, pesquisados ou comprados; c) demais usuários em situações semelhantes.⁹⁵

O aviso de privacidade da Amazon também trata especificamente de cookies, explicando que é possível desabilitar o uso dessas ferramentas no browser, mas, ao mesmo tempo, dizendo que “se você bloquear ou rejeitar nossos cookies, não será possível adicionar itens no seu carrinho, fazer o checkout e nem usar nenhum produto da amazon.com que requer que você sign in”. Dessa maneira, ainda que disponha que existe a possibilidade de desabilitar cookies, torna-se impossível fazê-lo e continuar usufruindo dos serviços da Amazon. Cabe ressaltar que existem diferentes tipos de cookies, com diferentes funcionalidades, seria tecnicamente possível distinguir os diferentes cookies e habilitar apenas aqueles que fossem essencialmente necessários para o funcionamento da plataforma.

C) DISPOSITIVOS VAGOS SOBRE SEGURANÇA E SIGILO DOS DADOS

A LGPD também traz dispositivos sobre medidas de segurança e sigilo de dados. É exigido dos controladores e operadores que sigam medidas técnicas e administrativas visando proteger “os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito” (artigo 46). Tais medidas de segurança devem abranger desde a fase de concepção do produto, até a sua execução. Violações em tal segurança devem ser comunicadas aos titulares dos dados que possam ser afetados por tal falha, mencionando, entre outros, os tipos de dados potencialmente afetados e as medidas tomadas para reverter a situação.

A lei ainda define que:

“Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as

94 MAGAZINE LUIZA. (2015). Política de Privacidade. Disponível em: <https://www.magazineluiza.com.br/politica/>

95 IDEM

obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais”.

Tal disposição incentiva que as empresas e entidades que tratem de dados pessoais instituem programas de governança em privacidade, criando uma cultura e normativas internas que prezam pela aplicabilidade adequada da lei e proteção dos titulares dos dados. Tais regras de boas práticas devem ser publicadas e atualizadas.

Contudo, as disposições sobre segurança nas políticas de privacidade analisadas são genéricas e geralmente tendem apenas e se eximir da culpa em relação ao vazamento de dados. A Social Miner, por exemplo, dispõe em sua política de privacidade que “opera com os mais altos padrões de segurança de dados, mas não se responsabiliza por eventuais roubos de dados e invasões terceiras”⁹⁶. De forma a especificar seus padrões de segurança, a start-up simplesmente disponibiliza um link para página listando os certificados de conformidade que a Amazon Web Services, provável servidor usado pela empresa, possui em todo o mundo.

Como protegemos suas informações?

Todas as informações de dado pessoal que são processadas pela Social Miner são guardadas em servidores com altos padrões de **segurança**. Isso significa dizer que trazemos mais camadas de proteção às suas informações, tornando mais difícil a violação delas por terceiros.

Para mais informações, consulte:

<https://aws.amazon.com/pt/compliance/programs/>

Figura 1: Disposição sobre a Amazon Web Services; Fonte: Política de privacidade da Social Miner.

96 SOCIAL MINER. Política de Privacidade. Disponível em: <https://socialminer.com/privacidade.html>

Ou seja, a empresa não explica o que significa possuir altos padrões de segurança com clareza e se exime da responsabilidade em relação aos danos potenciais oriundos de invasões. A LGDP não permite tal disposição.

O iFood, por sua vez, possui termos um pouco mais detalhados para se referir à segurança no tratamento dos dados. A política de privacidade diz que:

*“Só tratamos os seus dados mediante alto grau de segurança, implementando as melhores práticas em uso na indústria para a proteção de dados, tais como técnicas de criptografia, monitoramento e testes de segurança periódicos. Contudo, não é possível garantir completamente a não ocorrência de interceptações e violações dos sistemas e bases de dados do iFood, uma vez que a internet possui sua estrutura de segurança em permanente aperfeiçoamento”.*⁹⁷

Assim, mesmo que haja ligeira clareza em relação ao que a empresa entende como segurança, o iFood não se compromete ou propõe salvaguardas para seus clientes em caso de vazamentos ou violações que exponham os usuários. Ambos, Social Miner e iFood, sequer dispõem claramente sobre a comunicação aos usuários em casos de violação, evidente descumprimento da LGDP.

No ponto de segurança dos dados, a política de privacidade do Magazine Luiza traz uma consideração sobre a impossibilidade de se ter um sistema de segurança completamente seguro e, em função disso, afirma que a empresa se exime de “quaisquer responsabilidades por eventuais danos e/ou prejuízos decorrentes de falhas, vírus ou invasões do banco de dados do site, salvo nos casos de dolo ou culpa pela mesma.”⁹⁸ O documento em questão é bastante defasado em consideração com a LGPD que traz, em seu artigo 46⁹⁹, novos parâmetros de segurança das bases de dados que devem ser adotadas pelos agentes de tratamento a fim de proteger os usuários. Desta maneira, assim como no caso da Amazon, aqui caberia

97 IFOOD.(2018). Política de Privacidade. Disponível em: <https://www.ifood.com.br/privacidade>

98 MAGAZINE LUIZA. (2015). Política de Privacidade. Disponível em: <https://www.magazineluiza.com.br/politica/>

99 Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

uma adequação na política de privacidade da empresa uma vez que a LGPD não permite tal exceção da culpa.

Na central de privacidade, página da operadora Vivo, temos um aviso a respeito de eventuais situações em que nossas informações podem ser compartilhadas. Seria o caso de “ordens judiciais e solicitações de autoridades competentes”, em conformidade com a lei brasileira. Nesse caso, a empresa menciona que “registros de conexão, voz e dados” poderão ser disponibilizados sem nosso conhecimento. Na seção sobre segurança o portal da empresa afirma que utiliza criptografia no tráfego de informações dos nossos computadores para os servidores da vivo, ou seja, que utiliza https em suas páginas, mas nada menciona sobre criptografia de servidores. O portal também afirma que a empresa tenta se pautar pelos princípios da “confidencialidade” permitindo acesso aos dados apenas à pessoas autorizadas; “integridade”, tentando preservar a confiabilidade dos dados; “disponibilidade” para que informações sejam disponibilizadas quando necessário; e “auditabilidade”. Por fim, traz também algumas dicas de segurança para clientes.

Já a Privacy Notices da Amazon afirma apenas que usa certificado SSL na transmissão de informações, diz que revela apenas 4 últimos dígitos do cartão de crédito ao confirmar um pedido e sugere que clientes protejam suas senhas de uso não autorizado, incluindo um link ensinando como deslogar da conta. Ou seja, não temos nada muito específico sobre como os dados coletados pelo uso do Amazon Prime Video são armazenados, nem que medidas de segurança são tomadas por parte de ambas as empresas.

D) DIREITO DE ACESSAR COM FACILIDADE, CORRIGIR OU DELETAR INFORMAÇÕES

A LGDP também garante ao titular o direito de acessar com facilidade informações sobre a finalidade do tratamento dos dados, a duração e forma de tal tratamento, as informações sobre o controlador dos dados e sobre o compartilhamento deles com terceiros.

Há disposições na política de privacidade da Social Miner em relação ao compartilhamento com terceiros e finalidade dos dados, mas não é clara a duração do armazenamento dos dados dos usuários, tampouco há disposições detalhando como usuários podem demandar correções ou que seus dados sejam apagados da base.

Já o iFood afirma que poderá armazenar os dados enquanto seja necessário para os fins da política de privacidade e cumprimento dos termos de uso, “respeitando o período de retenção de dados determinado pela legislação aplicável”.¹⁰⁰ Também afirma que usuários poderão solicitar a exclusão da conta, mas não demonstram como tal pedido pode ser feito.

100 IDEM.

Em todo caso, dispõe que:

*“Em alguns casos, (o Ifood poderá) reter suas informações mesmo que você exclua sua conta, tais como nas hipóteses de guarda obrigatória de registros previstas na lei aplicável, se houver uma questão não resolvida relacionada à sua conta (como, por exemplo, uma reclamação ou disputa não resolvida), ou caso seja necessário para nossos interesses comerciais legítimos, como prevenção de fraudes e aprimoramento da segurança dos nossos usuários”.*¹⁰¹

A retenção de dados para interesses comerciais legítimos abre espaço para muitas possibilidades, posto o termo vago utilizado, e pode gerar armazenamentos onerosos e abusivos para os usuários. Além disso, feedbacks enviados por clientes sobre as entregas do iFood podem ser usados, segundo a política, para fins de publicidade e publicados no site e aplicativo da plataforma. Não se sabe, no entanto, se há clareza para o usuário da visibilidade irrestrita de seus feedbacks para além da disposição na política de privacidade.

O Magazine Luiza trata o usuário como o titular de fato dos dados e permite a adição, exclusão ou modificação de informações ligadas ao seu perfil de usuário¹⁰². Apesar do documento dispor sobre a garantia do direito do usuário de acessar, corrigir ou deletar suas informações, ele não menciona quais meios existentes poderão ser utilizados para a garantia do direito. Ainda sobre este ponto, a política de privacidade não trata da possibilidade de exclusão dos dados após o término da relação que motivou a coleta e tampouco o período de tratamento dos dados pessoais do usuário.

Já no caso da Amazon Prime Video, a Privacy Notice diz que podemos acessar informações sobre nossa conta “com o propósito limitado de visualizá-las” e, em alguns casos, atualizá-las. O documento também diz que podemos ver alguns exemplos, mas o link nos direcionou novamente para o Privacy Notice. Novamente, vemos com apreensão o fato do serviço de streaming não ter uma política de privacidade específica, pois o processo de profiling para um serviço de streaming de vídeos é distinto, por exemplo, do profiling feito para compra e venda de produtos. Atentamos para casos como o apontado por artigo do New York Times¹⁰³ que, ao investigar o sistema de recomendações e busca do Youtube no Brasil, demonstrou que a plataforma tende a direcionar usuários para canais de extrema direita. É preciso, portanto, pensar em que tipo de transparência podemos cobrar, desse e de outros tipos de serviços streaming que, cada vez mais, utilizam-se de inteligên-

101 IFOOD. (2018). Política de Privacidade. Disponível em: <https://www.ifood.com.br/privacidade>

102 MAGAZINE LUIZA. (2015). Política de Privacidade. Disponível em: <https://www.magazineluiza.com.br/politica/>

103 NEW YORK TIMES, “How Youtube radicalizes Brazil”, August, 11th, 2019: <https://www.nytimes.com/2019/08/11/world/americas/youtube-brazil.html>

cia artificial para fazer recomendações. Por fim, também não achamos nada que mencionasse explicitamente a possibilidade de exclusão de dados.

E) PRÁTICA DE PROFILING E POTENCIAL DE DISCRIMINAR POR ALGORITMOS

Com relação às práticas de profiling, a LGPD não é muito clara. Em seu artigo 5º, a lei traça definições de Dado Pessoal, Dado Pessoal sensível e Dado Anonimizado¹⁰⁴ e descreve que anonimização de dados é a utilização de “meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo”. Além disso, a lei autoriza o tratamento de dados pessoais para a realização de estudos por órgão de pesquisa, sempre que possível a anonimização das informações (art. 7º, inciso IV).

Outro ponto importante é que a LGPD não considera dados anonimizados como dados pessoais a não ser que o processo de anonimização possa ser revertido¹⁰⁵. O mesmo artigo 12 descreve que poderão ser considerados dados Pessoais aqueles utilizados para formação de perfis comportamentais de pessoa natural, se identificada, e que cabe à Autoridade Nacional de Proteção de Dados Pessoais dispor sobre “padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança”.

104 Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

105 Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

§ 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

Nesse sentido, caso as práticas de profiling trabalhem com dados anonimizados, elas não representam uma violação da LGPD. Adicionalmente, a Lei não define o que seriam os “esforços razoáveis e por meios próprios”¹⁰⁶ aplicáveis aos processos de reversão dos processos de anonimização e nem padrões mínimos para as empresas.

Em termos gerais, não foi possível concluir se a atividade das empresas analisadas no presente estudo influíam em práticas de profiling ou eventuais discriminações geradas por decisões algorítmicas.

A política de privacidade do iFood afirma que a empresa realiza uma classificação dos clientes conforme eventos realizados. Por exemplo, classificam usuários que “pedem mais determinada categoria de comida ou que realizam mais de 4 pedidos por mês”¹⁰⁷. Não se sabe, no entanto, quais usos específicos e detalhados de tais classificações, que podem gerar vulnerabilidade para os usuários na medida em que oferecem parâmetros claros de preferências e costumes pessoais que, cruzados com outras informações, podem ser sensíveis em relação à privacidade.

A operação da Social Miner, por sua vez, é baseada na análise do comportamento de compra do usuário feita automaticamente pelo algoritmo de inteligência artificial da start-up. No entanto, não há indicações sobre o funcionamento de tal algoritmo e das potenciais categorizações de usuários em grupos conforme padrão de compras, o que, mais uma vez, deixa o usuário em situação de vulnerabilidade e potencial superexposição. A empresa afirma fazer estudos sobre os padrões dos consumidores. Nesse caso, “tais dados terão as informações pessoais dos usuários deletadas, não se configurando mais um dado pessoal, e sim um mero conjunto de dados anônimos para fins de estudo e pesquisa”¹⁰⁸. Ainda assim, indica que há, em alguma medida, a criação de perfis conforme dados dos usuários.

A política de Privacidade da Magalu também é omissa com relação a eventuais práticas de profiling praticadas pela empresa e estratégias de direcionamento de conteúdo ou clusterização de clientes. Tudo o que o documento menciona é a eventual utilização de um cookie que identifica a navegação do Usuário para a posterior recomendação de produtos que será diferenciada para cada comportamento dentro do site. O documento também menciona que a recomendação de produtos será “gerada a partir de algoritmos, sua precisão pode não ser exata, porém visa sugerir produtos que sejam do interesse do Usuário, sem que este tenha qualquer obrigatoriedade de adquiri-los.”

O Amazon Prime Video tem contratado especialistas de análise de dados para melhorar seu algoritmo, mas seus termos de

106 SOARES, P. S. C. (2019). Anonimização na Lei Geral de Proteção de Dados requer posição da ANPD. Conjur. Disponível em: https://www.conjur.com.br/2019-mar-10/pedro-soares-anonimizacao-lei-geral-protECAo-dados#_ftn3

107 IFOOD.(2018). Política de Privacidade. Disponível em: <https://www.ifood.com.br/privacidade>

108 SOCIAL MINER. Política de Privacidade. Disponível em: <https://socialminer.com/privacidade.html>

serviço e política de privacidade não dizem muito sobre como isso funciona e nem qual nosso poder de intervir. Até porque as políticas de privacidade são genéricas e dizem respeito a todos os serviços da Amazon, e não especificamente ao Amazon Prime Video. Na política específica, temos apenas menção ao software, dizendo que ele pode fornecer à Amazon:

“(...) informações relativas ao seu uso e à performance do Serviço e do Software, assim como informações referentes aos dispositivos nos quais você baixa e utiliza o Serviço e o Software. Por exemplo, o Software poderá fornecer à Amazon informações relativas ao Conteúdo Digital que você baixa ou acessa via streaming e o seu uso desse Conteúdo Digital (como, por exemplo, se você visualizou um Conteúdo Digital e quando fez isso, o que poderá, entre outras coisas, nos ajudar a medir o Período de Acesso para Conteúdo Digital Alugado).” Mas não há informação sobre como esses dados são utilizados e nem sobre o poder do consumidor de editar diretamente o perfil que a Amazon o atribui.”

F) OUTRAS QUESTÕES ABORDADAS PELA LGPD

Além disso, a lei traz disposição específica sobre o tratamento de dados pessoais de crianças e adolescentes. Para tal, segundo a LGPD, se faz necessário o consentimento específico de um dos pais ou responsáveis legais. A exceção se dá quando “a coleta for necessária para contatar os pais ou o responsável legal”, devendo ser utilizada “uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento” (artigo 14, parágrafo 3).

Considerando a importância de se atentar para a transferência internacional de dados, dado que muitos recursos e aplicações da Internet transitam por países e legislações muito diversas, a LGPD defende que tal transferência apenas poderá ocorrer “para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto (na) Lei” e “quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos (na) Lei” (artigo 33 incisos 1 e 2). Ou seja, a lei brasileira segue padrão já adotado pelo regulamento europeu (GDPR) permitindo a transferência apenas para países que possuam salvaguardas similares ao padrão brasileiro de proteção dos dados.

Há exceção para tal norma, como por exemplo, quando a transferência é necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência e de persecução, ou quando for necessária para a proteção da vida ou da segurança física do titular ou de terceiro. Ainda assim, considerando as atividades cotidianas de empresas que lidam com dados, o

padrão a ser seguido é aquela da GDPR: transferência apenas para países de regulamentos similares.

Especificamente em relação aos controladores e operadores, ou seja, a quem compete as decisões sobre o tratamento de dados pessoais e quem as potencialmente executa em nome do controlador, a LGDP afirma que ambos precisam manter registro das operações que realizam, de forma a guardar memória do tratamento dos dados. Tal memória deve conter, no mínimo, “a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados” (artigo 39, parágrafo único).

Caso haja dano patrimonial, moral, individual ou coletivo em razão do tratamento dos dados pessoais, os controladores e/ou operadores são obrigados a repará-lo, segundo medidas judiciais. Além disso, a lei deixa claro que “o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador” e que “os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente” (artigo 42, parágrafo 1, incisos 1 e 2), inclusive quando o dano decorre de descuido de ambos em relação à adoção de medidas adequadas de segurança.

IV. AVALIAÇÃO DA ADEQUAÇÃO DO REGIME JURÍDICO PARA AS DINÂMICAS PRÓPRIAS DA ERA DIGITAL

A seção anterior traçou paralelos entre a atuação das empresas analisadas e a lei de proteção de dados pessoais no Brasil. Naturalmente, restam questões pouco ou indevidamente abordadas pela LGDP. Sobretudo a partir do insumo coletado na apresentação dos resultados preliminares da pesquisa para atores de distintos setores interessados, identificamos que a legislação nacional, centrada na LGDP, é focada na relação entre os titulares dos dados e os prestadores diretos de serviço. No entanto, o caso da Social Miner evidencia que nem sempre é assim e que, talvez, seria interessante um cuidado mais granular em relação às formas como os usuários têm seus dados coletados e explorados.

Outro ponto que levanta preocupações é a aplicação escalonada da Lei geral de Proteção de Dados Pessoais para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclararem startups ou empresas de inovação prevista como uma das competências da Autoridade Nacional de Proteção de dados Pessoais. De acordo com o artigo 55-J, inciso XVIII, cabe a ANPD editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para a adequação destas empresas ao disposto na Lei. No entanto, a previsão de uma aplicação mais relativizada pode gerar inseguranças para os cidadãos uma vez que estas empresas - conforme demonstrado na análise da atuação da Social Miner e da IFOOD - representam agentes relevantes no cenário de tratamento de dados pessoais a quem não cabe uma aplicação escalonada da lei.

Ademais, caberá a Autoridade Nacional de Proteção de Dados o papel de propor políticas simplificadas e diferenciadas para as micro e pequenas empresas, de forma a evitar competição inadequada e a redução da inovação. Ainda assim, até a elaboração de normas específicas, resta incerteza em relação à aplicação devida da lei.

De igual forma, é previsto em lei que o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses. Incluídas estão as decisões que visam definir perfil pessoal, profissional, de consumo e de crédito ou outros aspectos. Ainda assim, caberá à ANPD detalhar as regras que afetarão esse direito. Até lá, práticas que vimos na análise que são comuns às empresas baseadas em dados poderão sofrer com a fragilidade jurídica em relação ao profiling efetuado através de decisões automáticas.

Considerando que a autoridade de proteção de dados no país não foi estabelecida com a independência almejada, pode carcer ainda salvaguardas ao próprio Estado enquanto ente vigilante. Tal autoridade, no fim das contas, deterá informações

sobre o tratamento de dados de usuários de todo o país. Afinal, a DPA brasileira funcionará como um PROCON, visando atender aos anseios de consumidores? Como uma Agência Brasileira de Inteligência (ABIN), explorando seu conhecimento para potencialmente vigiar e armazenar informação privilegiada? A seção a seguir tratará mais detidamente sobre a autoridade.

V. AVALIAÇÃO DA CAPACIDADE DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS PARA LIDAR COM AS EMPRESAS SELECIONADAS

A Autoridade Nacional Proteção de Dados Pessoais Brasileira - ANPD - foi aprovada por ventura da sanção da Lei 13.583 de 8 de Julho de 2019, 11 meses depois da aprovação da Lei Geral de Proteção de Dados Pessoais. No entanto, o modelo de Autoridade de Proteção de Dados Pessoais adotado pelo Brasil ficou longe do desejado por alguns setores envolvidos na discussão da Lei uma vez que o órgão fará parte da Administração Pública direta e ligado à Casa Civil da Presidência da República.

Cumprir destacar que, as discussões relacionadas à aprovação da Lei de Proteção de Dados no Congresso Nacional envolveram um modelo de autoridade independente, com autonomia decisória, institucional e financeira, capaz de implementar e acompanhar a aplicação da Lei. A legalidade da criação da ANPD, como uma Autarquia, foi um ponto bastante questionado uma vez que as especificidades do modelo foram inseridas no texto da Lei no decorrer do debate legislativo. Os argumentos em torno da ausência de legalidade na criação da ANPD na discussão da lei influenciaram a decisão do Poder Executivo, que entendeu que o Congresso Nacional estava violando competência exclusiva da Presidência da República para legislar sobre a organização da Administração Pública Direta e Indireta e acabou vetando os dispositivos referentes à ANPD.

No entanto, no dia 27 de dezembro de 2018, foi editada a Medida Provisória n. 869/2018 que ao ser sancionada como Lei 13853/2019 alterou a Lei de Proteção de Dados e inseriu no texto da LGPD previsão de criação da ANPD como órgão da administração pública federal integrante da Presidência da República, reconhecendo que os vetos representavam *“risco de insegurança jurídica para a Sociedade Civil em face da falta de definição do órgão responsável pela regulação, controle e fiscalização da aplicação da Lei.”*¹⁰⁹

Após sua tramitação em comissão especial do Congresso Nacional, a ANPD foi aprovada e sancionada como o *“órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.”*

Ao órgão, a ser instituído âmbito do Poder Executivo *“sem criação de despesas”*, compete, de acordo com o Art. 55-J, sempre almejar alcançar uma tutela efetiva da privacidade dos cidadãos e, ao mesmo tempo, trazer mais segurança jurídica na

109 PRESIDÊNCIA DA REPÚBLICA DO BRASIL. (2018). Exposição de Motivos da Medida Provisória 869/2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Exm/Exm-MP-869-18.pdf

aplicação desta para os atores regulados, sejam eles do setor público ou privado. Um resumo de suas funções é a) fiscalizar o cumprimento da lei de proteção de dados; b) fiscalizar e aplicar sanções; c) apreciar petições de titulares de dados (cidadãos) contra os controladores; d) promover informação sobre políticas de proteção de dados e medidas de segurança; e) elaborar estudos; f) estimular adoção de serviços “privacy friendly”; g) cooperar com autoridades de proteção de dados de outros países; g) solicitar informes e dispor sobre formas de publicizar operações de tratamento; h) fazer estudos e editar regulamentos; i) realizar auditorias ou determinar sua realização; j) comunicar infrações à autoridades competentes.

A ANPD fica também responsável pela elaboração de diretrizes para uma Política Nacional de Proteção de Dados Pessoais e Privacidade, fiscalização das atividades de tratamento de dados pessoais e aplicação de eventuais sanções a agentes que violem os direitos estabelecidos na lei.

Vale mencionar que, no decorrer do debate legislativo, foi inserido no rol de competências da autoridade a previsão de:

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

Ou seja, o legislador tentou prever uma espécie de escalonamento da aplicação da Lei para startups e empresas disruptivas. O desafio apresentado para a ANPD, portanto, é a delimitação de regras e prazos para a adequação de startups que equilibrem o Direito à Privacidade e Proteção de Dados com o fomento à inovação sem enfraquecer o regime jurídico recém conquistado.

A Lei, em seu artigo 52, dispõe sobre as sanções aplicáveis aos agentes de tratamento de Dados, dispostas abaixo, e que não substituem a aplicação de sanções administrativas, civis ou penais em legislação específica.

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

Ao mesmo tempo que a criação de uma Autoridade de Proteção de Dados Pessoais é um fato importantíssimo para o cumprimento da Lei, vale destacar que o arranjo institucional para o exercício do poder de fiscalização não é ideal, conforme apontou Bruno Bioni em entrevista para o Jornal O Estado de São Paulo.

A recepção das sanções administrativas dispostas acima somente foi possível ante a reapreciação de vetos presidenciais pelo Congresso Nacional. No entanto, cumpre destacar que o grupo de sanções mais “severas” não pode ser revertido e o texto da lei ficou sem as seguintes previsões:

X- Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

XI - Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; e

XII - Proibição parcial ou total do exercício de atividades relacionada a tratamento de dados”.¹¹⁰

De acordo com o texto da Lei, a aplicação das sanções administrativas descritas acima só ocorreria ante a reincidência de uma determinada empresa ou entidade da administração pública. Ou seja, a aplicação dos dispositivos somente poderia ocorrer após a imposição de ao menos uma sanção administrativa dentre as descritas no rol do artigo 52 ou em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos estes órgãos.

110 CONGRESSO NACIONAL. (2019). Medida Provisória n. 869/2018. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7966761&ts=1563991644604&disposition=inline>

Importante mencionar que as sanções acima descritas eram fundamentais para fortalecer o poder de fiscalização e controle da Autoridade Nacional de Proteção de Dados Pessoais, uma vez que uma autoridade forte, com poder de sanção reforçado torna-se relevante para coibir abusos cometidos por agentes de tratamento de dados pessoais. No entanto, pode-se dizer que o modelo de autoridade a ser implementado no Brasil será insuficiente, uma vez que o órgão já nasce desprovido de autonomia - a lei garante autonomia técnica e decisória, mas a financeira e institucional ainda ficam pendentes a uma eventual revisão.

Inegavelmente, o modelo de regulação brasileira é bastante inspirado no modelo europeu - General Data Protection Regulation - que tem figurado como o grande exemplo de regime jurídico capaz de combater as violações dos direitos dos titulares de dados pessoais praticados pelas empresas do grupo GAFAM e da economia digital. No entanto, o debate legislativo brasileiro e as limitações de orçamento impossibilitaram que o Brasil atingisse um modelo de autoridade independente, com autonomia financeira e decisória, ponto adotado por várias autoridades de proteção de dados pessoais instituídas pelo mundo e fundamental para o funcionamento pleno da lei.

Ainda sobre o ponto da autonomia e independência da ANPD, o paliativo encontrado e inserido no texto foi a inclusão de dois parágrafos no texto da Lei, que indicam que a natureza jurídica do órgão poderá ser transformada pelo Poder Executivo em autarquia e que essa avaliação deverá ocorrer em até dois anos depois de agosto de 2020 (data da entrada em vigor da Lei).¹¹¹

O tamanho da ANPD também se mostra bastante modesto, composta por um conselho diretor, com cinco membros, e um Conselho Nacional de Proteção de Dados Pessoais e Privacidade com 23 integrantes. No entanto, a estrutura da ANPD ainda é desconhecida ao passo que a lei apenas informa que o órgão contará com uma Corregedoria, Ouvidoria, órgão de assessoramento jurídico próprio e eventuais unidades administrativas e unidades especializadas necessárias à aplicação da Lei (art. 55-C).

A proposta de autoridade ganha com a criação do Conselho Nacional de Proteção de Dados Pessoais (art. 58-A). O órgão multissetorial composto por 23 representantes do Setor Público, Privado, terceiro setor e academia, permite uma participação mais efetiva dos setores interessados na atividade da ANPD. De acordo com a Lei (art. 58-B), o CNPD fica responsável por (a) elaborar diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados

111 Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República.

§ 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República.

§ 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD.

Pessoais e da Privacidade e para a atuação da ANPD; (b) elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; (c) elaborar estudos e realizar debates e audiências públicas; e (d) disseminar o conhecimento.

Desta maneira, torna-se necessário o debate com o Poder executivo a respeito da transformação da ANPD em Autarquia tendo em vista que o simples vínculo da autoridade nacional com a administração pública é um fator que a enfraquece. No modelo atual, o órgão fica desprovido de autonomia administrativa e, portanto, sujeita a eventuais controles políticos e obstáculos para a investigação de práticas ilegais de agentes de tratamento de dados públicos ou até privados. Somente com uma entidade regulatória com independência financeira e institucional, dotada de um corpo técnico altamente profissionalizado, que a lei poderá ser concretizada.

Por fim, ressaltamos que, ante a crise instaurada pela Pandemia de COVID-19, iniciada após a conclusão do estudo, foi fortalecido o coro em torno de uma possível postergação da *vacatio legis* da Lei no âmbito dos poderes Executivo e Legislativo. Até o presente momento, a discussão está sendo promovida no âmbito dos Projetos de Lei n. 5762/2019¹¹², n. 1179/2020¹¹³ e da recém proposta Medida Provisória n. 959/2020¹¹⁴. Entre os projetos de lei, o mais avançado é o 1179/2020, já aprovado pelo Senado e cujo substitutivo da Senadora Simone Tebet¹¹⁵ aguarda a apreciação da Câmara dos Deputados. No entanto, em 29 de abril de 2020, o Presidente da República enviou a MP 959/2020 ao Congresso Nacional, propondo, dentre outras coisas, a postergação da vigência para Maio de 2021.

Ante a urgente necessidade de criação da Autoridade Nacional de Proteção de Dados Pessoais e a aplicação de regras mais claras aos agentes de tratamento, entendemos que a postergação da entrada em vigor da Lei acaba por trazer mais insegurança jurídica e deixa de figurar como possível mecanismo de pressão para a criação da ANPD. Adicionalmente, com a mudança da *vacatio legis* - para Janeiro ou Maio de 2021 - os indivíduos ficam desprotegidos ante eventuais abusos do Direito à Privacidade cometidos neste cenário das novas dinâmicas sociais - e virtuais - introduzidas pelo Coronavírus¹¹⁶. Aqui, a LGPD é ferramenta garantidora do direito à privacidade e proteção de dados.

112 C MARA DOS DEPUTADOS. (2019). Projeto de Lei 5762/2019. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2227704>

113 SENADO FEDERAL. (2020). Projeto de Lei 1179/2020. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/141306>

114 CONGRESSO NACIONAL. (2020). Medida Provisória 959/2020. Disponível em: <https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141753>

115 O substitutivo apresentado pela Senadora Simone Tebet propõe dois novos prazos de *vacatio legis*: Janeiro de 2021 para a lei e Agosto de 2021 para as sanções administrativas.

116 A Coalizão Direitos na Rede, em posicionamento emitido em março de 2020, apontou que o Estado Brasileiro precisa respeitar o compromisso assumido com a Proteção de Dados Pessoais. O posicionamento pode ser encontrado aqui: <https://direitosnarede.org.br/2020/03/31/o-estado-brasileiro-precisa-respeitar-o-compromisso-assumido-com-a-protecao-de-dados-pessoais.html>

VI. CONCLUSÃO E RECOMENDAÇÕES

De uma maneira geral, práticas já conhecidas de empresas com modelos de negócios baseados em dados também foram identificadas nas empresas analisadas. Uso de cookies e outras formas de coleta de dados de navegação, compartilhamento de bases de dados com terceiros e direcionamento de conteúdo em plataformas por meio de profiling, de uma forma ou outra, foram identificados nas empresas analisadas pelo presente estudo. Além disso, como no caso Colombiano, também foi identificada uma forte relação com as empresas GAFAM, seja pela utilização de dados das plataformas para autenticação ou pela possibilidade de direcionamento de conteúdo nas mesmas.

Em relação às quatro empresas analisadas, a atual política de privacidade do Ifood e do Magazine Luiza foram escritas antes da sanção da LGDP e, portanto, não fazem menção à legislação ou às obrigações da lei de forma direta. De igual forma, a Social Miners também não menciona a LGDP, mas faz claras conexões com o regulamento europeu, afirmando estar de acordo com a norma europeia. Já a Vivo, que disponibiliza o Amazon Prime Video, inaugurou recentemente uma Central de Privacidade, que, de certa forma se alinha à princípios da LGPD, mas maior parte dos dados de utilização do serviço, são regidos pelo Aviso de Privacidade da Amazon, que não só não menciona a lei brasileira, como está disponível apenas em inglês.

Considerando o regime jurídico apresentado e a situação atual da autoridade nacional de proteção de dados, ainda é cedo para alegar que a regulação será forte o bastante para combater eventuais violações de privacidade e direitos dos cidadãos praticadas pelas empresas. A Autoridade Nacional de Dados Pessoais, no modelo aprovado, aparenta ser fraca e sem poder efetivo de fiscalização. Em função disso, para que a fiscalização dos agentes de tratamento de Dados Pessoais seja efetiva no país, é importante que o órgão esteja disposto a cooperar com outros setores e órgãos fiscalizadores como os pertencentes ao Sistema nacional de Defesa do Consumidor e a própria Justiça Federal.

Por isso, recomenda-se:

PARA OS AGENTES DE TRATAMENTO DE DADOS ANALISADOS:

1. A atualização de todas as políticas de privacidade e termos de uso para gerar harmonização com a Lei Geral de Proteção de Dados. As empresas precisam se adequar tanto em vocabulário, quanto em ação à lei brasileira, buscando deixar mais claro para o usuário seus direitos garantidos por lei e os detalhes do tratamento de seus dados pessoais. Resta incompleta, por exemplo, a política da Social Miner, que cita a normativa europeia em sua política de privacidade várias vezes, mas sem lidar diretamente com a legislação brasileira que logo vigorará em todo território nacional.

2. A disponibilização das políticas de privacidade e dos termos de uso de forma facilitada, integrada e traduzida para a língua portuguesa. Por exemplo, houve dificuldade em entender qual política de privacidade rege os serviços da Amazon Prime Video quando contratada pela Vivo. É essencial que empresas forneçam, conforme disposto em lei, informações claras, suficientes e de fácil acesso aos seus clientes ou clientes em potencial, se são duas empresas envolvidas, seria fundamental um único documento que deixasse claro para o consumidor o papel de cada uma no tratamento de seus dados.

3. A disponibilização e indicação, nos termos de uso e políticas de privacidade, de mecanismos e/ou contato para usuários que desejem obter mais informações referentes ao tratamento de seus dados. Mesmo que a LGDP disponha sobre a possibilidade dos usuários demandarem informações ou modificações sobre o tratamento de seus dados, ainda resta incerto, nas políticas analisadas e, acredita-se, em grande parte das EMNDB, um caminho claro a ser tomado pelo usuário sempre que ele desejar fazer uso de seus direitos assegurados pela LGDP.

4. A instauração de políticas de governança. Em nenhuma das quatro empresas analisadas, foram encontradas diretrizes que apontassem para medidas de governança ou princípios orientadores do tratamento dos dados e cuidado com a segurança dos usuários. A LGPD recomenda que as empresas sejam transparentes quanto aos seus processos internos de gestão de dados, mas não houve, até o momento nas empresas analisadas, clara execução de tal recomendação.

5. O detalhamento, por parte das empresas, acerca das medidas de segurança adotadas. Algumas empresas usaram termos vagos para se referir ao tema, outras até mesmo se eximiram da responsabilidade de ressarcir os usuários em caso de vazamentos e violações.

6. É necessária maior investigação sobre o panorama de atuação das empresas com modelos de negócios baseados em dados no país a partir de sua incidência sobre os direitos e liberdades dos cidadãos. Sobretudo considerando a iminência da aplicação da lei, é vital para usuários e para as próprias empresas que haja material em português e focado especificamente no contexto brasileiro sobre a relação entre as normas incidentes sobre a proteção de dados pessoais e a atuação de empresas. Tais estudos poderão, inclusive, ser utilizados pela ANPD quando ela iniciar suas operações, de forma a construir um conhecimento técnico e embasado em empiria sobre o tema.

7. O uso de cookies e outros trackers também precisa ser entendido e tratado com mais detalhes, para que não se interprete, por padrão, que os dados que coletam são anonimizados, e, portanto, fora do âmbito de proteção da lei, como pudemos ver afirmados em algumas políticas de privacidade.

8. Deve-se observar que, por vezes, na relação com as empresas GAFAM, dados sensíveis estão sendo coletados, mas não encontramos menção a dados sensíveis em nenhuma política de privacidade.

9. Também sugerimos que opt-in para determinadas coletas de dados seja o padrão, ao invés de opt-out, o que tem sido comum nos termos analisados.

10. Por fim, é necessário mais clareza e transparência sobre as práticas de profiling das empresas, tema que não apareceu claramente explicitado em nenhuma das políticas de privacidade ou termos de uso.

COM RELAÇÃO À AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS E A LEI BRASILEIRA DE PROTEÇÃO DE DADOS PESSOAIS

11. A criação da Autoridade Nacional de Dados Pessoais e sua posterior transformação em autarquia, pertencente à Administração Pública Indireta - conforme previsto na lei. Uma autoridade com independência técnica e financeira, e com forte poder de fiscalização é necessária para garantir a tutela dos direitos dos usuários e aplicar sanções mais severas aos agentes de tratamento de dados pessoais.

12. Que a vigência da Lei Geral de Proteção de Dados não seja mais adiada. A entrada em vigor da lei fornecerá mais segurança jurídica para atuação das empresas analisadas no presente estudo, ao passo que fomenta a criação de estruturas internas de adequação à Lei. Adicionalmente, uma lei vigente e aplicável é necessária para a proteção dos cidadãos ante eventuais abusos dos agentes de proteção de dados pessoais.

REFERÊNCIAS

- AMAZON. (2017). Amazon Privacy Notice. Disponível em: <https://www.amazon.com/gp/help/customer/display.html?nodeId=468496>
- AMAZON PRIME VIDEO. (2019). Termos de Uso do Amazon Prime Video. Disponível em: <https://www.primevideo.com/region/na/help?nodeId=202095490>
- App Store. App do Magazine Luiza. Disponível em: <https://apps.apple.com/br/app/magazine-luiza-comprar-online/id891130066>
- BASSETTE, F. (2017). A estratégia por trás do vídeo viral do Magazine Luiza. Veja. Disponível em: <https://veja.abril.com.br/blog/virou-viral/estas-vendedoras-da-magazine-luiza-estao-enlouquecendo-a-internet/>
- BARBOSA, V. (2018). Até a mascote virtual do Magazine Luiza é alvo de assédio sexual. Revista Exame. Disponível em: <https://exame.abril.com.br/marketing/ate-a-mascote-virtual-do-magazine-luiza-e-alvo-de-assedio-sexual/>
- BELLONI, L. (2018). Como o iFood se tornou o maior aplicativo de delivery de comida da América Latina. Huffington Post. Disponível em: https://www.huffpostbrasil.com/2018/04/18/como-o-ifood-se-tornou-o-maior-aplicativo-de-delivery-de-comida-da-america-latina_a_23414651/
- BLOOMBERG. (2017), Magazine Luiza usa Tinder pra ampliar vendas e tem alta de 2000%. Jornal O Globo. Disponível em: <https://oglobo.globo.com/economia/magazine-luiza-usa-tinder-pra-ampliar-vendas-tem-alta-de-2000-21705034>
- BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm
- _____. Lei 12.965, de 23 de Abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm
- _____. Lei 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/L13709.htm

_____. Lei 13.583, 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

_____. Medida Provisória n. 869, de 27 de dezembro de 2018. 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/_ato2015-2018/2018/Mpv/mpv869impressao.htm

BRIGATTO, G. (2018). Mobile investe US\$ 500 milhões no iFood e planeja criar líder global. Valor Econômico. Disponível em: <https://www.valor.com.br/empresas/5983273/mobile-investe-us-500-milhoes-no-ifood-e-planeja-criar-lider-global>

CALADO, C. (2018). Magazine Luiza – entrevista com o time responsável pela criação da Lu. Medium Bots Brasil. Disponível em: <https://medium.com/botsbrasil/magazine-luiza-entrevista-com-o-time-respons%C3%A1vel-pela-cria%C3%A7%C3%A3o-da-lu-8fc987fbafad>

CÂMARA DOS DEPUTADOS. (2019). Projeto de Lei 5762/2019. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2227704>

COALIZÃO DIREITOS NA REDE. (2020). O Estado Brasileiro precisa respeitar o compromisso assumido com a Proteção de Dados Pessoais. Disponível em: <https://direitosnarede.org.br/2020/03/31/o-estado-brasileiro-precisa-respeitar-o-compromisso-assumido-com-a-protecao-de-dados-pessoais.html>

CONGRESSO NACIONAL. (2020). Medida Provisória 959/2020. Disponível em: <https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141753>

CONGRESSO NACIONAL. (2019). Medida Provisória n. 869/2018. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7966761&ts=1563991644604&disposition=inline>

DAROIT, G. (2019). iFood quer seguir entregando crescimento. Jornal do Comércio. Disponível em: https://www.jornaldocomercio.com/_conteudo/cadernos/empresas_e_negocios/2019/05/685035-ifood-quer-seguir-entregando-crescimento.html

ESTADÃO. (2018). Mulher virtual da Magazine Luiza reclama de assédio em comentários. O estado de S. Paulo. Disponível em: <https://emails.estadao.com.br/noticias/comportamento,mulher-virtual-da-magazine-luiza-reclama-de-assedio-em-co>

mentarios,70002484761

FRAGA, N. (2018). “Temos de ajudar o consumidor na inclusão digital”, diz Trajano, do Magazine Luiza. Época Negócios. Disponível em: <https://epocanegocios.globo.com/Empresa/noticia/2018/02/fabio-coelho-do-google-e-luiza-trajano-do-magazine-luiza-conversam-sobre-inclusao-digital.html>

FREITAS, T. (2019). As 8 startups brasileiras de machine learning que serão aceleradas pelo Google. Startse. Disponível em: <https://www.startse.com/noticia/startups/61939/8-startups-brasileiras-launchpad-accelerator>

FREITAS, T. (2019). iFood registra 17,4 milhões de pedidos no mês de março. Startse. Disponível em: <https://www.startse.com/noticia/startups/63248/ifood-atinge-a-marca-174-milhoes-de-pedidos-no-mes-de-marco>

GARTENBERG, C. (2019). YouTube is back on the Fire TV, and Prime Video launches on Chromecast starting today. The Verge. Disponível em: <https://www.theverge.com/2019/7/9/20686773/youtube-fire-tv-prime-video-chromecast-amazon-google-launch-today-available>

GAZZONI, M E CRUZ, P. (2011). Luiza Trajano: do balcão da loja dos tios a ministra do governo. Último Segundo - iG. Disponível em: <https://ultimosegundo.ig.com.br/politica/luiza-trajano-do-balcao-da-loja-dos-tios-a-ministra-do-governo/n1597158849986.html>

GHELFI, R. e CAPELAS, B. (2019). Governo sanciona MP que cria Autoridade Nacional de Proteção de Dados. O Estado de S. Paulo. Disponível em: <https://link.estadao.com.br/noticias/geral,governo-sanciona-mp-que-cria-autoridade-nacional-de-protecao-de-dados,70002913612>

GOMES, M. C. O. (2018). Cookie notice: informar, obter e por fim coletar dados pessoais. (JOTA). Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/cookie-notice-informar-obter-e-por-fim-coletar-dados-pessoais-23112018>

Google Play Store. App do Magazine Luiza. Disponível em: https://play.google.com/store/apps/details?id=com.luizalabs.mlapp&hl=pt_BR

HIGA, P. (2019). Fim da briga: YouTube volta ao Fire TV e Prime Video estreia no Chromecast. Tecnoblog. Disponível em: <https://tecnoblog.net/297901/youtube-volta-fire-tv-prime-video-chromecast/>

IFOOD. Cidades Atendidas. Disponível em: <https://www.ifood.com.br/cidades-atendidas>

_____. (2013). Termos de Uso. Disponível em: <https://www.ifood.com.br/termos>

_____. (2018). Política de Privacidade. Disponível em: <https://www.ifood.com.br/privacidade>

JESUS, A. (2012). Magazine Luiza lança F-commerce no Facebook e Orkut. Techtudo. Disponível em: <https://www.techtudo.com.br/noticias/noticia/2012/02/magazine-luiza-faz-sucesso-com-seu-f-commerce-no-facebook-e-orkut.html>

LIMA, L. (2017). iFood lança chatbot para pedir pizza no Messenger, mas será se funciona?. Novarejo. Disponível em: <https://portalnovarejo.com.br/2017/07/ifood-chatbot-messenger/>

LINKEDIN. Head of Subscription Video Analytics, Prime Video US. Amazon Job post at Linkedin. Disponível em: <https://www.linkedin.com/jobs/view/head-of-subscription-video-analytics-prime-video-us-at-amazon-1094636760/>

LETIERI (2019). Usuários colocam iFood no sobrenome e não conseguem mudar. Techtudo. Disponível em: <https://www.techtudo.com.br/noticias/2019/05/usuarios-colocam-ifood-como-sobrenome-no-facebook-e-nao-conseguem-mudar.ghml>

LUNA, D. (2018). MP do DF abre inquérito contra Vivo por suspeita de uso de dados pessoais. O estado de S. Paulo. Disponível em: <https://link.estadao.com.br/noticias/empresas,mp-do-df-abre-inquerito-contravivo-por-suspeita-de-uso-de-dados-pessoais,70002253400>

MAGAZINE LUIZA. (2015). Política de Privacidade. Disponível em: <https://www.magazineluiza.com.br/politica/>

_____. Canal da Lu - Magalu. Youtube. Disponível em: <https://www.youtube.com/user/MAGAZINELUIZACOM>

_____. (2019). E-commerce do Magazine Luiza cresce 56% no segundo trimestre Em menos de três anos, faturamento do Marketplace chega a ¼ das vendas digitais. Release. Disponível em: <https://ri.magazineluiza.com.br/Download/magalurelease2T19--1-?=lart1882KdnmVEwBwRdEmQ==&idcanal=rqFYRysdRDkTGGc93mpXJg==>

_____. Quem Somos. Disponível em: <https://ri.magazineluiza.com.br/ShowCanal/Quem-Somos?=urUqu4hANldyCLgMRgOsTw==>

MANZONI Jr, R. (2017). Como o Magazine Luiza pretende enfrentar a Amazon? Istoé Dinheiro. Disponível em: <https://www.istoed.com.br/2017/07/20/como-o-magazine-luiza-pretende-enfrentar-a-amazon-istoed-dinheiro/>

istoedinheiro.com.br/como-o-magazine-luiza-pretende-enfrentar-amazon/

MEIO E MENSAGEM. (2018). Amazon Prime Video e Viacom anunciam conteúdo original. Disponível em: <https://www.meioemensagem.com.br/home/ultimas-noticias/2018/11/14/viacom-negocia-series-para-amazon-prime-video.html>

MONTEIRO, R. L. (2017). "Proteção de dados e a legislação vigente no Brasil". Baptista Luz. Disponível em: <http://baptista-luz.com.br/wp-content/uploads/2017/11/Privacy-Hub-Leis-Setoriais.pdf>

OGILVY & MATHER BRASIL. (2019). Missão Digital Magazine Luiza. Disponível em: <http://www.ogilvy.com.br/cases/missao-digital>

OLIVEIRA, F. (2019). Hackers aproveitam erro de digitação em campanha do iFood para infectar consumidores com vírus. Folha de S. Paulo. Disponível em: <https://www1.folha.uol.com.br/mercado/2019/03/hackers-aproveitam-erro-de-digitacao-em-campanha-do-ifood-para-infectar-consumidores-com-virus.shtml>

ORACLE. (2018). New Startups Join Oracle Startup Cloud Accelerator to Enhance Cloud Innovation. Disponível em: <https://www.oracle.com/br/corporate/pressrelease/startup-accelerator-brazil-second-cohort-2018-06-07.html>

ORRICO, A. (2018). Tem uma galera dando em cima da vendedora virtual da Magazine Luiza. Buzzfeed. Disponível em: <https://www.buzzfeed.com/br/alexandreorrico/vendedora-virtual-da-magazine-luiza>

PEGN. (2018). As 100 startups brasileiras para ficar de olho. Disponível em: <https://revistapegn.globo.com/Startups/noticia/2018/04/100-startups-brasileiras-para-ficar-de-olho.html>

PRESIDÊNCIA DA REPÚBLICA DO BRASIL. (2018). Exposição de Motivos da Medida Provisória 869/2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Exm/Exm-MP-869-18.pdf

PRIVACY INTERNATIONAL. (2019). State of Privacy Brazil. Disponível em: <https://privacyinternational.org/state-privacy/42/state-privacy-brazil>

RICCIARDI, A. (2016). Como Frederico Trajano está mudando os rumos do Magazine Luiza. Forbes. Disponível em: <https://forbes.uol.com.br/negocios/2016/07/como-frederico-trajano-esta-mudando-os-rumos-do-magazine-luiza/>

SALOMÃO, K. (2017). "Não tiro a barriga do balcão", diz Luiza Helena Trajano. Exame. Disponível em: <https://exame.abril.com.br/empresas/luiza-helena-trajano-nao-tiro-a-barriga-do-balcão/>

com.br/negocios/nao-tiro-a-barriga-do-balcao-diz-luiza-helena-trajano/

SENADO FEDERAL. (2020). Projeto de Lei 1179/2020. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/141306>

SOCIAL MINER. Política de Privacidade. Disponível em: <https://socialminer.com/privacidade.html>

_____. Política de Cookie. Disponível em: <https://socialminer.com/cookies.html>

_____. Sobre Nós. Disponível em: <https://socialminer.com/sobre-nos.html>

Portal da Social Miner. Disponível em: <https://socialminer.com/>

_____. Cases de Sucesso. Disponível em: <https://socialminer.com/>

_____. (2018). “O comportamento do consumidor Online em 2018”. Disponível em: https://conteudo.socialminer.com/relatorio-comportamento-do-consumidor?utm_source=ECBR&utm_medium=artigo&utm_campaign=relatorio-comportamento-do-consumidor-2018

_____. (2018). Social Miner no Oracle Startup Cloud Accelerator. Disponível em: <http://blog.socialminer.com/people-marketing/social-miner-no-oracle-startup-cloud-accelerator/>

SOARES, P. S. C. (2019). Anonimização na Lei Geral de Proteção de Dados requer posição da ANPD. Conjur. Disponível em: https://www.conjur.com.br/2019-mar-10/pedro-soares-anonimizacao-lei-geral-protecao-dados#_ftn3

SOUSA, G. (2019). Páginas Falsas da Magalu no Facebook Tentam Roubar Dados. Adnews. Disponível em: <https://adnews.com.br/internet/paginas-falsas-da-magalu-no-facebook-tentam-roubar-dados/>

SOUZA, B. (2016). Como a Social Miner usa inteligência artificial, mas também gente, para inovar no marketing digital. Projeto Draft. Disponível em: <https://projetodraft.com/como-a-social-miner-usa-inteligencia-artificial-mas-tambem-gente-para-inovar-no-marketing-digital/>

SPOONROCKET. Site do Serviço Spoonrocket: <https://www.spoonrocket.com.br/>

VIVO. (2018). Termos de Uso do Serviço Amazon Prime Video. Disponível em: http://ws.mobile.terra.com/Descargas/Storage/0000000000/062000/062250/Terms62250_PT_20181008133419.pdf

____. Centro de privacidade. Disponível em: https://www.vivo.com.br/portalweb/appmanager/env/web?_nfls=false&_nfpb=true&_pageLabel=vivoVivoInstPrivacidadePage&WT.ac=portal.amarca.privacidade&#

VIVO. Vivo para sua casa. Disponível em: https://www.vivoparasuacasa.com.br/amazonprimevideo/?gclid=EAIaIQobChMllba8weX_4wIVIIaRCh3epwrjEAAAYASAAEgKRlvD_BwE

VELOSO, T. (2012). Magazine Luiza lança programa de comissão para Facebook. Tecnoblog. Disponível em: <https://tecnoblog.net/74606/magazine-luiza-facebook/>

ZUINI, P. (2013). Movable investe R\$ 5,5 milhões na iFood. Exame. Disponível em: <https://exame.abril.com.br/pme/movable-investe-r-5-5-milhoes-na-ifood/>

ANEXOS - VERSÃO DOS TERMOS DE USO E POLÍTICAS DE PRIVACIDADE ANALISADAS PARA ESSA PESQUISA

I. Política de Privacidade - iFOOD

II. Termos e Condições - iFOOD

III. Política de Privacidade - Social Miner

IV. Política de Cookies - Social Miner

V. Política de Privacidade - Magazine Luiza

VI. Termos de Uso do Amazon Prime Video

VII. Amazon Privacy Notice

VIII. Termos e Condições de uso - específico para assinatura do prime video pelas clientes Vivo

IX. Termo de Tratamento de Dados Pessoais da Telefônica

ANEXO I. POLÍTICA DE PRIVACIDADE - IFOOD

Data de atualização: 17 de julho de 2018

Versão Anterior: [Acesse aqui](#)

Nós utilizamos os seus dados como parte da nossa missão de proporcionar um serviço cada vez melhor. Essa política descreve como obtemos, armazenamos, utilizamos e compartilhamos as suas informações.

A proteção dos seus dados e da sua privacidade são muito importantes para o iFood. Portanto, recomendamos que você conheça melhor as nossas práticas e, em caso de dúvidas, entre em contato conosco.

Você consente, de forma livre e expressa, que seus dados e informações sejam coletados, armazenados, tratados e compartilhados, conforme as regras dispostas nesta Política de Privacidade.

Ao se cadastrar no iFood, o Usuário garante de forma expressa que é plenamente capaz, nos termos da legislação vigente, para exercer e gozar de todos os Serviços. Ademais, os Usuários menores de 18 anos deverão obter o consentimento expresso de seus pais, tutores ou representantes legais para utilizar os Serviços, conforme as disposições dos Termos e da Política de Privacidade do iFood. Os pais, tutores ou representantes legais serão plenamente responsáveis também no caso de acesso ao iFood por parte de crianças e adolescentes, sem a devida obtenção de autorização prévia. Cabe a eles a integral responsabilidade pela fiscalização das atividades e conduta dos respectivos menores sob sua tutela, bem como ciência da integralidade dos presentes Termos.

Informamos ainda a você que o serviço prestado pelo iFood não é direcionado a adolescentes e crianças menores de 13 anos.

Quais tipos de informações coletamos?

Como utilizamos essas informações?

Como utilizamos cookies e outras tecnologias?

Como as informações são armazenadas?

O iFood transfere os dados para outros países?

Como as informações são compartilhadas?

Como respondemos a requerimentos legais?

Como protegemos suas informações?

Como iremos notificá-lo em caso de mudanças à essa política?

Como entrar em contato com iFood em caso de dúvidas?

Quais tipos de informações coletamos?

Ao utilizar o Website ou Aplicativo de propriedade do iFood, nós coletamos algumas informações importantes para que possamos prestar um serviço adequado para você. Abaixo detalhamos quais são essas informações.

INFORMAÇÕES QUE VOCÊ NOS FORNECE

Quando você se inscrever para ser um usuário registrado do iFood, poderemos obter uma série de informações sobre você, tais como: seu nome, data de nascimento, CPF, endereço eletrônico, endereço de correspondência, senha, número de telefone e preferências de contato.

Para criar o seu cadastro no Website ou Aplicativo do iFood, você pode ainda usar a sua conta em redes sociais. Por exemplo, ao utilizar o Facebook para se inscrever no nosso serviço, você estará permitindo que o iFood acesse as informações pessoais em sua conta do Facebook, tais como seu nome, e-mail, gênero, idade e telefone (caso o tenha cadastrado no Facebook). As informações que poderemos obter, nesse caso, dependem das suas configurações de privacidade junto ao serviço de rede social.

Você tem a opção de importar seus contatos pessoais (incluindo as informações disponíveis no serviço de rede social) para o nosso serviço, permitindo assim que você localize seus amigos e seus amigos o localizem.

Além dessas informações iniciais de cadastro, você pode ainda nos fornecer dois tipos de informações: (a) dados de pagamento (apenas nos casos em que o pagamento é online); (b) informações de localização e (c) informações dos seus dispositivos. Abaixo detalhamos essas informações.

A. INFORMAÇÕES DE PAGAMENTO

Ao fazer o seu pedido pelo iFood, é possível que, a depender do restaurante escolhido, você possa fazer o pagamento diretamente no nosso aplicativo.

Ao escolher fazer o pagamento direto no nosso Website ou Aplicativo, você poderá nos fornecer os seus dados de pagamento, tais como aqueles de cartão de crédito e de meios de pagamento parceiros

Nós usamos esses dados para poder confirmar a sua ordem de pagamento e garantir que não ocorram fraudes por meio dos nossos Serviços.

B. INFORMAÇÕES DE LOCALIZAÇÃO

Para poder realizar a entrega do seu pedido, nós precisamos que você também nos informe a sua localização ou a localização do local em que gostaria que entregássemos o seu pedido.

Essa localização pode ser fornecida pelo endereço que você inserir manualmente no aplicativo, ou através da localização obtida do seu dispositivo via GPS e redes móveis (torres de celular, Wi-Fi e outras modalidades de localização) e confirmada por você.

Para fins da lei nº 12.965 de 2014 (Marco Civil da Internet), ou qualquer lei que venha substituí-la, a localização fornecida será considerada como dado cadastral.

C. INFORMAÇÕES DOS SEUS DISPOSITIVOS

Além dessas informações que você mesmo nos fornece, nós podemos coletar algumas informações automaticamente sobre os dispositivos a partir dos quais você acessa o iFood.

Dentre essas informações estão endereços IP, tipo de navegador e idioma, provedor de serviços de Internet (ISP), páginas de consulta e saída, sistema operacional, informações sobre data e horário, dados sobre a sequência de cliques, fabricante do dispositivo, operadora, modelo, redes Wi-Fi, número de telefone, entre outras que poderão ser coletadas pelo iFood.

INFORMAÇÕES NÃO-PESSOAIS

Nós também podemos obter informações não-pessoais, ou seja, dados que não permitem a associação direta com qualquer pessoa especificamente. São exemplos de dados não-pessoais a idade do indivíduo, preferências individuais, idioma, CEP e código de área.

Nós também poderemos obter informações sobre as atividades dos usuários no nosso Website ou Aplicativo. Essas infor-

mações são agregadas e usadas para nos ajudar a fornecer informações para os nossos clientes e entender quais partes dos nossos produtos e serviços atraem mais interesse dos usuários. Dados agregados são considerados informações não-pessoais para fins desta Política de Privacidade.

Se combinarmos informações não-pessoais com informações pessoais, a informação combinada será tratada como informação pessoal enquanto essa informação permanecer combinada.

COMO UTILIZAMOS ESSAS INFORMAÇÕES?

PROMOVER, MELHORAR E DESENVOLVER NOSSOS SERVIÇOS

Podemos usar essas informações coletadas para nos ajudar a desenvolver, oferecer e melhorar os nossos produtos e serviços destinados a você, existentes ou serem criados.

Também poderemos usar suas informações pessoais para fins internos, tais como auditoria, análise de dados e pesquisas para aprimorar os produtos, serviços e comunicações com os clientes, e geração de análises estatísticas com respeito ao uso dos nossos serviços, incluindo tendências de consumo.

AVALIAÇÃO DE RESTAURANTES

Ao enviar comentários e feedback com relação ao Website ou Aplicativo e os serviços de delivery dos nossos parceiros, você nos autoriza a publicar e utilizar tais comentários e feedbacks no Website ou Aplicativo e em quaisquer materiais de marketing ou publicidade, bem como a analisar, processar e tratar esse feedback de forma isolada ou agregada nos termos desta política de privacidade. Para tanto, apenas identificaremos você através de seu nome de cadastro, foto do perfil do iFood (caso você tenha uma) e da sua cidade de residência.

COMUNICAÇÃO

Periodicamente poderemos usar suas informações pessoais para enviar avisos e notificações importantes, como comunicados sobre compras, alterações em prazos, condições e políticas. Como estas informações são importantes para a sua interação com o iFood, você não poderá optar por não receber esse tipo de comunicação, já que são inerentes ao uso do serviço.

SEGURANÇA

Nós podemos também utilizar esses dados coletados para aprimorar a segurança e melhorar os serviços e as ofertas do iFood destinadas a você. Dessa forma, podemos analisar e solucionar problemas técnicos, bem como identificar e coibir fraudes na utilização do nosso Serviço.

MARKETING

Nós poderemos usar suas informações pessoais para enviar publicidade, bem como outros materiais promocionais voltados ao marketing de nossos serviços e de novidades para você, o que inclui campanhas digitais (tais como marketing direcionado em redes sociais e notificações push) e não digitais (como divulgação em radiodifusão, outdoors, panfletos, entre outros).

Nesse caso, você pode optar por não receber mais e-mails de marketing a qualquer momento, alterando as suas preferências.

Além disso, poderemos compartilhar as informações com parceiros do iFood, para fins de desenvolver campanhas de marketing mais relevantes para interessados nos produtos do iFood. O iFood somente compartilhará dados com parceiros que possuem política de privacidade que ofereça níveis compatíveis de proteção àquele oferecido por esta política.

PROMOÇÕES

Se você participar de um concurso, competição ou qualquer outra modalidade de promoção, poderemos usar as informações que você fornecer para administrar esses programas.

DADOS NÃO-PESSOAIS

Nós poderemos usar informações não-pessoais para a consecução das finalidades previstas nessa Política de Privacidade.

COMO UTILIZAMOS COOKIES E OUTRAS TECNOLOGIAS?

O iFood se utiliza de tecnologias como cookies, pixel tags, armazenamento local ou outros identificadores, tanto de dispositivos móveis ou não, ou tecnologias semelhantes (“cookies e outras tecnologias”), para uma variedade de funções. Essas tecnologias nos ajudam a autenticar a sua conta, promover e aperfeiçoar os serviços do iFood, personalizar a sua experiên-

cia e avaliar a eficácia da nossa comunicação e publicidade.

O QUE SÃO ESSAS TECNOLOGIAS?

Cookies são pequenos arquivos armazenados no seu navegador, celular ou outro dispositivo.

Pixel tags (ou GIFs limpos, web beacons ou pixels) são pequenos blocos de código em uma página da web que permitem que elas realizem ações como ler e armazenar cookies e transmitir informações para o iFood. A conexão resultante pode incluir informações como o endereço de IP de um dispositivo, a hora em que uma pessoa visualizou o pixel, um identificador associado ao navegador ou dispositivo e o tipo de navegador em uso.

Identificadores de dispositivo mobile são códigos que possibilitam a identificação do seu dispositivo mobile, seja de maneira persistente ou transitória, tais como o ID de Publicidade ou o ID de seu sistema operacional.

Armazenamento local é uma tecnologia padrão da indústria que permite que um website ou aplicativo armazene e recupere dados do computador, celular ou outro dispositivo de uma pessoa. Exemplos desse mecanismo são HTML5 e caching.

COMO FUNCIONAM?

Cookies e outras tecnologias nos ajudam a melhor prestar os nossos serviços a você, bem como a entender melhor o seu comportamento, nos dizendo quais partes de nosso Website ou Aplicativo as pessoas visitaram e, ainda, facilitam a medição da eficácia da publicidade e das pesquisas na web.

Nós tratamos as informações obtidas por meio de cookies e outras tecnologias como informações não-pessoais. Entretanto, na medida em que o endereço protocolo de internet (endereço IP) ou identificadores semelhantes sejam considerados informações pessoais pela lei local aplicável, nós também trataremos esses identificadores como informação pessoal.

Da mesma forma, na medida em que a informação não-pessoal seja combinada com informação pessoal, nós tratamos a informação combinada como informação pessoal para os fins desta Política de Privacidade.

Você pode gerenciar as suas preferências de cookies e outras tecnologias semelhantes a partir da configuração de seu navegador ou dispositivo, recusando ou excluindo determinados cookies e outras tecnologias. Contudo, isso poderá comprometer a prestação dos nossos serviços ou impedir o funcionamento de determinadas funcionalidades que os integram.

Os nomes específicos dos cookies e outras tecnologias usados podem variar à medida em que os nossos serviços são

melhorados e atualizados, mas eles geralmente se restringem às categorias de uso abaixo:

CATEGORIAS DE USO / EXEMPLOS / AUTENTICAÇÃO

Indica que você está conectado, para que seja possível oferecê-lo os recursos apropriados, bem como para entender como você usa nossos serviços.

SEGURANÇA E INTEGRIDADE

Ajuda a manter a segurança dos nossos serviços, oferecendo suporte ou ativando recursos de segurança e ajudando a detectar atividades que violam nossos Termos e Condições de Uso e Política de Privacidade. Por exemplo, auxilia a proteger a sua conta contra acessos indesejados.

ANÚNCIOS, IDEIAS E MEDIÇÃO

Ajuda a analisar comportamentos de navegação, a fim de veicular e medir anúncios, torná-los mais relevantes para você e analisar o conteúdo e uso de produtos e serviços. Por exemplo, é possível usar um cookie ou outra tecnologia para descobrir se alguém que tenha sido exposto a um anúncio realiza uma compra relacionada ao anúncio.

RECURSOS E SERVIÇOS

Ajuda a fornecer produtos e serviços. Por exemplo, quando você vê ou interage com conteúdo dos nossos serviços, é possível oferecer a você outros plug-ins sociais, diferentes experiências e conteúdo personalizado.

DESEMPENHO

Ajuda a proporcionar a melhor experiência possível, por exemplo, ajudando a rotear o tráfego entre servidores e perceber com que velocidade o serviço do iFood é carregado para diferentes pessoas. Ocasionalmente, poderão ser armazenadas informações no seu navegador ou dispositivo para que os recursos em uso carreguem e respondam rapidamente.

ANÁLISES E PESQUISAS

Ajuda a entender, aprimorar e pesquisar produtos e serviços quando você acessa o iFood.

Promover uma experiência personalizada

O iFood e os seus parceiros também usam cookies e outras tecnologias para memorizar informações pessoais quando você usa o nosso Website, Aplicativo ou a rede de parceiros do iFood que possam usar tecnologias similares. A nossa meta nesses casos é fazer com que a sua experiência com o iFood seja mais conveniente e personalizada.

Por exemplo, saber o seu primeiro nome nos permite dar boas-vindas a você na próxima vez em que você acessar o iFood. Conhecer seu país e idioma nos permite viabilizar a você uma experiência de compras personalizada e mais útil. Saber que você adquiriu determinado produto ou usou um determinado serviço permite fazer com que sua publicidade e comunicações de e-mail sejam mais relevantes para os seus interesses.

Nessa linha, podemos também usar essas informações para classificar os usuários dentro da rede iFood, identificando os usuários a partir de eventos realizados, como a primeira compra ou o download do nosso aplicativo, e a partir de determinadas características de seu perfil, como usuários que pedem mais determinada categoria de comida ou que realizam mais de 4 pedidos por mês.

AVALIAR A EFICÁCIA DA NOSSA COMUNICAÇÃO E PUBLICIDADE

Nós usamos essas informações também para entender e analisar tendências, administrar os nossos serviços, aprender sobre o comportamento do usuário e obter informações demográficas sobre a nossa base de usuários de maneira geral. Em algumas de nossas mensagens de e-mail, nós usamos uma “URL click-through” (endereço externo) vinculada ao conteúdo do iFood. Quando os clientes clicam em uma dessas URLs, os usuários são enviados para um servidor diferente antes de chegarem à página de destino no nosso serviço.

Nós monitoramos esses dados de click-through para entender o interesse em determinados tópicos e avaliar a eficácia das comunicações com os nossos clientes. Se você preferir não ser monitorado dessa maneira, não clique em texto ou links contidos em mensagens de e-mail enviadas pelo iFood.

Os pixel tags nos permitem enviar mensagens de e-mail em formatos que os usuários possam ler e nos dizer se o e-mail foi aberto ou não. Nós podemos usar essas informações para reduzir ou eliminar as mensagens enviadas aos usuários.

TECNOLOGIA DE TERCEIROS

Além dos cookies e outras tecnologias do iFood, nós podemos permitir que terceiros contratados pelo iFood utilizem coo-

kies e outras tecnologias de sua propriedade para identificar seu navegador e dispositivo, de modo a lhe oferecer publicidade direcionada do iFood quando você acessa websites ou aplicativos de terceiros.

Esses terceiros podem também fornecer ao iFood informações acerca do desempenho das campanhas de marketing desenvolvidas.

algumas dessas empresas podem utilizar cookies e outras tecnologias próprios nos serviços do iFood, tais como: Facebook Google Analytics e Double Click.

COMO AS INFORMAÇÕES SÃO ARMAZENADAS? ONDE AS INFORMAÇÕES SÃO ARMAZENADAS?

As informações que coletamos de você são armazenadas em serviços de nuvem confiáveis de parceiros que podem estar localizados no Brasil ou em outros países que ofereçam serviço de armazenamento de nuvem confiáveis e usualmente utilizados por empresas de tecnologia, tais como Estados Unidos da América (EUA) e em países da América Latina e da Europa.

Na contratação desses serviços, o iFood sempre busca empresas que empregam alto nível de segurança no armazenamento de suas informações, estabelecendo contratos que não violam as definições de privacidade previstas nessa Política.

POR QUANTO TEMPO AS INFORMAÇÕES SÃO ARMAZENADAS?

O iFood armazena as suas informações durante o período necessário para as finalidades apresentadas nos Termos e Condições de Uso do iFood e nesta Política de Privacidade, respeitando o período de retenção de dados determinado pela legislação aplicável..

Caso você solicite a exclusão de sua conta, as suas informações pessoais fornecidas ao iFood durante a sua utilização dos nossos serviços serão excluídos definitivamente sempre que a legislação assim o exigir.

Em alguns casos, poderemos reter suas informações mesmo que você exclua sua conta, tais como nas hipóteses de guarda obrigatória de registros previstas na lei aplicável, se houver uma questão não resolvida relacionada à sua conta (como, por exemplo, uma reclamação ou disputa não resolvida), ou caso seja necessário para nossos interesses comerciais legítimos, como prevenção de fraudes e aprimoramento da segurança dos nossos usuários.

O IFOOD TRANSFERE OS DADOS PARA OUTROS PAÍSES?

O iFood poderá realizar transferências internacionais de dados para outros países, tais como Estados Unidos da América e para países da União Europeia e da América Latina, a fim de realizar algumas das atividades envolvidas nos serviços prestados a você, bem como para poder obter informações que possam contribuir para o aperfeiçoamento dos nossos serviços.

Em qualquer caso de compartilhamento com parceiros localizados em outros países, estabelecemos contratualmente que o parceiro possua padrão de proteção de dados e segurança da informação compatível com esta política de privacidade, a fim de que seus dados sejam sempre protegidos nestes termos.

COMO AS INFORMAÇÕES SÃO COMPARTILHADAS?

Além das finalidades descritas acima, nós podemos também compartilhar com terceiros as suas informações coletadas em algumas hipóteses, que descreveremos abaixo.

PARA OUTROS USUÁRIOS DO IFOOD

Quando você se inscreve nos nossos serviços e submete suas informações pessoais para criar um perfil ou coleção visual, outros usuários verão seu nome e foto.

Caso você tenha optado por fornecer informações pessoais adicionais em seu perfil, os usuários do iFood também verão essas informações adicionais, incluindo, mas não se limitando a, website e informações biográficas. Fornecer informação adicional é uma opção sua. Nós recomendamos que você proteja e não divulgue na internet nenhuma informação que você considere sensível ou confidencial.

COM EMPRESAS DO GRUPO IFOOD

Nós podemos compartilhar os dados que coletamos com as empresas do Grupo Econômico ao qual pertence o iFood (“Grupo do iFood”).

As empresas do Grupo do iFood seguem o mesmo padrão de proteção de dados pessoais descrito nesta Política de Privacidade do iFood e obedecem às mesmas finalidades descritas neste documento. Ao compartilharmos os seus dados essas empresas, as mesmas garantias e cuidados que o iFood possui com os seus dados serão replicados pelas empresas do Grupo do iFood.

O compartilhamento de dados com empresas do Grupo do iFood terá como finalidades: (a) o desenvolvimento de novos produtos e serviços; (b) a oferta de produtos e serviços que melhor atendam aos seus interesses; (c) geração de dados estatísticos e agregados acerca do uso de nossos produtos e serviços e perfis dos usuários.

EM ALTERAÇÃO DE CONTROLE SOCIETÁRIO DO IFOOD

No caso de operações societárias, como reestruturação, fusão ou venda de ativos do iFood, do grupo econômico ou de parte dele, seus dados poderão ser transferidos, desde que respeitados os termos desta política de privacidade.

PROVEDORES DE SERVIÇOS E OUTROS PARCEIROS

Por razões de processamento e inteligência em relação aos dados do iFood, poderemos também compartilhar informações com algumas empresas ou indivíduos prestadores de serviço ou empresas parceiras do iFood. Nesse caso, os dados serão tratados de forma a proteger a sua privacidade, tendo essas empresas dever de proteção compatível com o da política de privacidade do iFood.

Nós podemos utilizar os serviços dessas empresas para facilitar nosso serviço, prover o serviço do iFood em nosso nome, executar atividades relacionadas ao serviço, incluindo – mas não se limitando a –, manutenção dos serviços, transporte e entrega de compras realizados por você, gerenciamento de banco de dados, análise de dados e melhoria de funcionalidades incluindo marketing, ou auxiliar-nos na avaliação de como o nosso serviço é usado.

Em relação ao pagamento de suas compras no nosso Website ou Aplicativo, caso opte por pagar diretamente online, nós poderemos compartilhar seus dados de pagamento com empresas processadores de pagamento com os quais trabalhamos. Esse compartilhamento é feito com o fim exclusivo de viabilizar a compra efetivada por você.

Essas empresas ou indivíduos têm acesso à sua informação pessoal apenas para executar atividades solicitadas pelo iFood e são obrigados a não usar ou divulgar tais informações para nenhuma outra finalidade.

RESTAURANTES PARCEIROS DO IFOOD

Ao fazer um pedido em um restaurante parceiro pelo nosso Website ou Aplicativo, nós podemos compartilhar algumas informações suas com esse restaurante parceiro, bem como fornecer dados a respeito do pedido em específico. As informações compartilhadas podem incluir nome, número de telefone, endereço de entrega, CPF (quando for solicitado), entre outras.

SERVIÇOS DE REDES SOCIAIS E OUTROS PROVEDORES DE APLICAÇÃO

Nós podemos divulgar informações de sua conta no iFood (incluindo informações pessoais) para outros provedores de aplicação ligados à sua conta iFood. Nós permitimos que você conecte sua conta de serviços de redes sociais e outros provedores de aplicação aos serviços do iFood.

Dessa forma, você poderá postar atividades recentes em nossos serviços nas suas contas de redes sociais. Se você não quiser mais postar suas atividades em sua conta de rede social, poderá simplesmente fazer isso ou alterar suas preferências quando a opção estiver disponível.

PARA PUBLICIDADE E SERVIÇOS DE ANÁLISE

Para poder entregar publicidade e promoções adequadas para você, bem como aperfeiçoar nossos serviços, nós também podemos compartilhar as suas informações com empresas especializadas em marketing e análise de dados digitais que ofereçam nível de proteção de dados compatível com esta política de privacidade.

COMO RESPONDEMOS A REQUERIMENTOS LEGAIS?

O iFood também poderá compartilhar suas informações com autoridades policiais ou judiciais, autoridades públicas competentes ou outros terceiros, dentro e fora do país em que você reside, caso seja requerido pela legislação aplicável, por decisão judicial e por requisição de autoridades, ou se necessário para responder a processos judiciais ou para participar em eventuais litígios ou disputas de qualquer natureza.

Nestas situações, o iFood cooperará com as autoridades competentes na medida em que discricionariamente entenda necessário e adequado em relação a qualquer investigação de ilícitos, infrações a direitos de propriedade industrial ou intelectual, ou outra atividade que seja ilegal ou que possa expor o iFood ou seus usuários a qualquer responsabilidade legal ou lhes impor riscos, ressalvadas hipóteses de sigilo de informações constantes na legislação aplicável.

Além disso, o iFood se reserva o direito de compartilhar informações sobre seus usuários a terceiros quando houver motivos suficientes para considerar que a atividade de um usuário é suspeita, ilegal ou prejudicial ao iFood ou a terceiros.

Este direito será utilizado pelo iFood quando considerar apropriado ou necessário para manter a integridade e a segurança do seu serviço, para o cumprimento dos seus Termos e Condições de Uso e Política de Privacidade, e com o intuito de cooperar com a execução e cumprimento da lei, independentemente de existir ou não uma ordem judicial ou administrativa

para tanto.

COMO PROTEGEMOS SUAS INFORMAÇÕES?

O iFood emprega seus melhores esforços para respeitar e proteger suas informações pessoais contra perda, roubo ou qualquer modalidade de uso indevido, bem como contra acesso não autorizado, divulgação, alteração e destruição.

Utilizamos o moderno princípio de privacy by design, respeitando a sua privacidade e protegendo seus dados nos nossos processos internos como um todo.

Só tratamos os seus dados mediante alto grau de segurança, implementando as melhores práticas em uso na indústria para a proteção de dados, tais como técnicas de criptografia, monitoração e testes de segurança periódicos. Contudo, não é possível garantir completamente a não ocorrência de interceptações e violações dos sistemas e bases de dados do iFood, uma vez que a internet possui sua estrutura de segurança em permanente aperfeiçoamento.

COMO IREMOS NOTIFICÁ-LO EM CASO DE MUDANÇAS À ESSA POLÍTICA?

O iFood poderá atualizar essa Política de Privacidade periodicamente, sendo que a versão em vigor será sempre a mais recente.

Se fizermos alguma alteração na política em termos materiais, podemos colocar um aviso no nosso Website, Aplicativo ou te enviar um e-mail, juntamente com a Política de Privacidade atualizada. Por isso é sempre importante manter seus dados de contato atualizados.

Para verificar a data da versão em vigor, verifique a “Data de atualização” no início desse documento.

COMO ENTRAR EM CONTATO COM IFOOD EM CASO DE DÚVIDAS?

Se você tiver algum questionamento ou dúvida com relação à Política de Privacidade do iFood ou qualquer prática aqui descrita, entre em contato conosco no endereço através do e-mail privacidade@ifood.com.br. Para que sua solicitação seja devidamente analisada por nós, ela deverá conter, no mínimo, as seguintes informações:

Nome completo;

Tipo e número de documento de identificação;

Telefone para contato;

E-mail (o mesmo utilizado no cadastro do iFood);

Descrição da dúvida ou motivos de eventual solicitação.

ANEXO II. TERMOS E CONDIÇÕES - IFOOD

Por favor, leia com atenção os termos e condições. Ao se cadastrar no ifood.com.br você ESTÁ DE ACORDO COM AS CONDIÇÕES E TERMOS do Website. Note que a recusa destes Termos do Website impedirá que você faça pedidos de produtos do nosso Website.

1. SERVIÇOS OFERECIDOS

1.1 Este TERMO se aplica para regular o uso do serviço oferecido pelo ifood.com.br aos USUÁRIOS, qual seja, possibilitar a escolha, pelos USUÁRIOS, de RESTAURANTES cadastrados e, via on-line, efetivar solicitações para aquisição (e entrega em domicílio e retirada no local) de gêneros alimentícios fornecidos pelos RESTAURANTES, de acordo com o cardápio disponibilizado, sendo possível, igualmente, aos USUÁRIOS, a efetivação do pagamento do preço dos produtos via on-line.

1.2 O serviço do ifood.com.br consiste, portanto, em aproximar, através do nosso site, os USUÁRIOS e os RESTAURANTES cadastrados, possibilitando que os USUÁRIOS encaminhem, aos RESTAURANTES, pedidos de entrega de gêneros alimentícios, bem como, sendo essa a opção dos USUÁRIOS, receber on-line pagamento do preço dos produtos entregues aos USUÁRIOS pelos RESTAURANTES.

1.3 Desde logo fica esclarecido ao USUÁRIO - o qual se declara ciente - que o serviço oferecido pelo ifood.com.br se relaciona apenas à intermediação (com opção de pagamento on-line) para comercialização de produtos alimentícios, não abrangendo preparo, embalagem, disponibilização e entrega física (via motoboy ou outros meios) dos produtos, sendo esses quatro itens de responsabilidade integral do RESTAURANTE, a quem deverão ser direcionados quaisquer reclamos acerca de problemas decorrentes de vício, defeito ou inexecução da feitura, preparo e entrega de produtos alimentícios.

2. CADASTRO

2.1 O USUÁRIO, para utilizar os serviços acima descritos, deverá ter capacidade jurídica para atos civis e deverá, necessariamente, prestar as informações exigidas no CADASTRO, assumindo integralmente a responsabilidade (inclusive cível e criminal) pela exatidão e veracidade das informações fornecidas no CADASTRO, que poderá ser verificado, a qualquer momento, pelo ifood.com.br .

2.1.1 Em caso de informações incorretas, inverídicas ou não confirmadas, bem assim na hipótese da negativa em corrigi-las ou enviar documentação que comprove a correção, o iFood Delivery se reserva o direito de não concluir o cadastra-

mento em curso ou, ainda, de bloquear o cadastro já existente, impedindo o USUÁRIO de utilizar os serviços on-line até que, a critério do ifood.com.br, a situação de anomalia esteja regularizada. O ifood.com.br se reserva o direito de impedir, a seu critério, novos CADASTROS, ou cancelar os já efetuados, em caso de ser detectada anomalia que, em sua análise, seja revestida de gravidade ou demonstre tentativa deliberada de burlar as regras aqui descritas, obrigatórias para todos os USUÁRIOS. Também agirá o ifood.com.br de tal forma caso verifique descumprimento, pelo USUÁRIO, de qualquer obrigação prevista no presente TERMO.

2.2 Efetuado, com sucesso, o CADASTRO, o USUÁRIO terá acesso aos serviços por meio de login e senha, dados esses que se compromete a não divulgar a terceiros, ficando sob sua exclusiva responsabilidade qualquer solicitação de serviço que seja feita com o uso de login e senha de sua titularidade.

3. OBRIGAÇÕES DO USUÁRIO

3.1 Efetuado com sucesso o CADASTRO do USUÁRIO, este se obriga a não divulgar a terceiros login e senha de acesso, nem permitir o uso de tais informações por terceiros, responsabilizando-se pelas consequências do uso de login e senha de sua titularidade.

3.2 É obrigação do USUÁRIO fornecer informações cadastrais totalmente verídicas e exatas, responsabilizando-se exclusiva e integralmente (em todas as searas jurídicas) por todo o conteúdo por si informado no item CADASTRO, mantendo atualizado e confirmado o endereço para entrega dos produtos encomendados.

3.3 O USUÁRIO se obriga, também, a pagar integralmente o preço dos produtos por si solicitados ou encomendados ao RESTAURANTE e efetivamente a si entregues, seja pela modalidade on-line, seja por qualquer outra forma, diretamente ao portador dos produtos encomendados por meio deste site (dinheiro, cheque, tickets, etc.).

3.4 O USUÁRIO que seja menor de 18 anos de idade está ciente de que não poderá encomendar e adquirir, em qualquer hipótese, produtos alcoólicos, responsabilizando-se pela correta informação de sua idade no item CADASTRO.

3.5 O USUÁRIO concorda com o uso das informações de avaliações e feedbacks do serviços dos RESTAURANTES e do iFood, conforme descrito nos TERMOS DE PRIVACIDADE do iFood.

4. OBRIGAÇÕES DO IFOOD.COM.BR

4.1 Disponibilizar no site ifood.com.br espaço virtual que permita ao USUÁRIO devidamente cadastrado efetivar pedidos de

compra de gêneros alimentícios anunciados e comercializados pelos RESTAURANTES e, também, disponibilizar ao USUÁRIO meios de pagamento do preço dos produtos on-line.

4.2 Proteger, por meio de armazenamento em servidores ou quaisquer outros meios magnéticos de alta segurança, a confidencialidade de todas as informações e cadastros relativos aos USUÁRIOS, assim como valores atinentes às operações financeiras advindas da operacionalização dos serviços previstos no presente TERMO. Contudo, não responderá pela reparação de prejuízos que possam ser derivados de apreensão e cooptação de dados por parte de terceiros que, rompendo os sistemas de segurança, consigam acessar essas informações.

5. MODIFICAÇÕES DESTE TERMO

5.1 O presente TERMO DE USO poderá, a qualquer tempo, ter seu conteúdo, ou parte dele, modificados para adequações e inserções, tudo com vistas ao aprimoramento dos serviços disponibilizados.

5.2 As novas condições entrarão em vigência assim que sua veiculada no site, sendo possível ao USUÁRIO manifestar oposição a quaisquer dos termos modificados, desde que o faça por escrito, através do site ifood.com.br , o que gerará o cancelamento de seu CADASTRO.

6. CANAL DE COMUNICAÇÃO

6.1 Para estabelecer contato entre ifood.com.br e o USUÁRIO fica disponibilizado o endereço eletrônico deste link, sendo certo que o USUÁRIO se obriga, igualmente, a manter em seu cadastro endereço eletrônico atual por intermédio do qual se farão as comunicações a ele dirigidas pelo ifood.com.br , desde logo emprestando-se validade jurídica e efetividade a esse meio eletrônico de troca de informações recíprocas.

7. ACEITAÇÃO DO TERMO DE USO

7.1 O USUÁRIO declara ter lido, entendido e que aceita todas as regras, condições e obrigações estabelecidas no presente TERMO.

8. FORO DE ELEIÇÃO

8.1 As partes elegem como competente para dirimir eventuais controvérsias que venham a surgir da interpretação e do cumprimento do presente TERMO o foro da Comarca do São Paulo - SP.

Última atualização: 19 de março de 2013

ANEXO III. POLÍTICA DE PRIVACIDADE - SOCIAL MINER

A Social Miner tem como um dos seus pilares fundamentais o compromisso com a segurança de dados e privacidade do usuário final, bem como dos seus clientes, sempre embasada nas mais recentes normas nacionais e internacionais, como a GDPR. Através desse documento, vamos esclarecer todos os pontos relativos a coleta de dados, seja no nosso site ou na nossa plataforma (socialminer.com ou panel.socialminer.com)

Alertamos que se você não concorda com o conteúdo desta política, não é recomendável baixar nossos materiais em utilizar quaisquer de nossos serviços e, caso tenha baixado ou utilizado e queira exercer seus direitos de restrição, retificação, exclusão ou oposição, entre em contato pelo privacy@socialminer.com.

GLOSSÁRIO

Para melhor entendimento dos termos abaixo propostos, informa-se, como referencial, o significado das seguintes palavras ou expressões:

GDPR: General Data Protection Regulation. É a regulamentação sobre a coleta e processamento de dados pessoais feita pela União Europeia, que entrou em vigor em 25/05/2018.

Usuário: Por usuário, leia-se o visitante do site de um dos clientes da plataforma.

Visitante: Por visitante, entende-se ser aquele que visita nosso site, com o objetivo, ou não, de ser um futuro cliente da plataforma.

Cliente: Por cliente, leia-se aquele que possui contrato ativo com a Social Miner, utilizando-se de nossa plataforma para buscar um maior engajamento seus clientes e uma melhora em sua performance de vendas.

SOBRE A GDPR (GENERAL DATA PROTECTION REGULATION) E SEUS DIREITOS COMO USUÁRIO

Apesar de legalmente a GDPR não possuir força sobre as empresas que atuam no Brasil e não coletam dados de cidadãos europeus que residem em território europeu, a SOCIAL MINER tem como pilar fundamental o respeito aos princípios que regem a privacidade de dados dos usuários, conforme disposto na norma europeia. Visando trazer ainda mais transparência aos usuários, a SOCIAL MINER atua em concordância com a GDPR e, sendo assim, os visitantes que acessam nossos conteúdos, bem como os usuários dos clientes da plataforma, possuem os seguintes direitos:

- 1- Direito a ser informado: o usuário/visitante tem como direito ser informado sobre quais dados são processados e concordar com a coleta de seus dados.
- 2- Direito ao acesso das informações: o usuário/visitante tem o direito a ter acesso às informações coletadas e processadas pela SOCIAL MINER.
- 3- Direito à retificação: havendo quaisquer discrepâncias nas informações processadas, o usuário/visitante tem o direito de solicitar o ajuste de qualquer informação equivocada que fora armazenada.
- 4- Direito ao esquecimento: é direito do usuário/visitante pedir que se delete os dados até então armazenados, tendo efeitos retroativos, mas não futuros.
- 5- Direito ao processamento restrito: direito do usuário/visitante a que se processe o mínimo possível de informações para os fins aos quais se destina.
- 6- Direito a portabilidade de dados: o usuário/visitante tem o direito a ter acesso a seus dados em um formato possível de ser reutilizado para fins de portabilidade.
- 7- Direito à objeção: o usuário/visitante possui o direito de proibir a coleta de processamento de novos dados, ou seja, a restrição tem efeitos futuros.
- 8- Direitos em relação a tomadas de decisão automatizadas: o usuário/visitante pode, ainda, contestar decisões feitas por meio automatizados, ou elaboração de perfis, se tais decisões tiverem o poder de produzir efeitos jurídicos para si, ou outro efeito igualmente significativo.

Caso você, como visitante da nossa página, queira exercer quaisquer desses direitos, entre em contato conosco pelo privacy@socialminer.com, informando o motivo de sua comunicação. Para usuários dos clientes da plataforma, tal direito deve ser solicitado diretamente ao cliente, que deverá entrar em contato com a Social Miner informando a solicitação.

SOBRE A FORMA DE COLETA DE DADOS PESSOAIS DE VISITANTES PARA CADASTRO

Ao se conectar com nosso site, a Social Miner coleta informações de visitantes das seguintes formas:

Informações Fornecidas pelo visitante: sempre que um visitante fizer download de algum material educativo, realizar um cadastro no nosso site ou participar de algum webinar ou evento organizado pela Social Miner, pediremos informações como nome, e-mail, telefone, site da sua empresa, setor ou categoria de negócio e tráfego do site onde trabalha. Essas

informações serão usadas para contato pró-ativo do time de vendas e marketing da Social Miner. Em se tratando de download de materiais, caso o material tenha sido elaborado em parceria com terceiros, os dados de cadastro fornecidos no momento do download poderão ser disponibilizados a estes.

Informações de navegação e Facebook: caso o visitante esteja navegando pelos nossos sites ou plataforma, a visita será transformada em dado pelo nosso Google Analytics. Se o visitante optar por se conectar com a nossa marca via Facebook Login, suas informações públicas básicas, como nome, idade, sexo, bem como suas informações demográficas serão coletadas, mediante aprovação prévia, e serão cruzadas com seus dados de navegação, de forma a permitir uma maior personalização das mensagens enviadas pela nossa empresa. Essas informações serão usadas para contato pró-ativo do time de vendas e marketing da Social Miner.

Informações coletadas por opt-in: Ao navegar em algumas de nossas páginas, poderá ser dada a opção de conectar via opt-in, com uma notificação no canto superior ou inferior da tela. Nessa hipótese, poderá ser coletado, mediante consentimento do visitante, os dados de nome, e-mail, e informações de Cookie (para maiores informações sobre coleta de cookie, visite nossa página de Política de Cookies).

Todas as informações de contato são registradas no banco de dados da nossa própria plataforma, em plataformas terceiras de gerenciamento e nutrição de leads e CRM de vendas.

SOBRE A COLETA DE DADOS DOS USUÁRIOS PARA FORMAR A BASE DE LEADS DO CLIENTE

Quando alguém se torna um cliente da Social Miner, nós usamos plugins de conexão, em especial o Facebook Login, para criar uma base de usuários para a marca do cliente. Os avisos e telas de conexão poderão aparecer ao final da navegação de cada usuário ou ao início, quando o mesmo demonstrar intenção de sair do site do cliente, de forma a não prejudicar a navegação ou atrapalhar eventuais procedimentos de compra.

É importante ressaltar que, segundo as normas da GDPR, o cliente da nossa plataforma que vender para usuários europeus residentes na União Europeia, possui a obrigação de informar aos seus usuários que está coletando cookies para monitorar o comportamento do usuário e melhorar a experiência dele com o site, atendendo ao princípio da GDPR que garante o direito à informação, informando, ainda, que ao se conectar via redes sociais ou e-mail, estará se fazendo coleta de tais dados pessoais.

Caso o usuário opte por se conectar via “opt-in”, ou seja, por notificações do navegador, poderemos coletar, mediante consentimento, dados como nome, e-mail, e demais informações de Cookie (para maiores informações sobre coleta de cookie,

visite nossa página).

Caso o usuário opte por se conectar com a sua marca via Facebook Login, suas informações públicas básicas, como nome, idade, sexo, bem como as informações demográficas serão coletadas mediante aprovação prévia do usuário, e serão cruzadas com seus respectivos dados de navegação, de forma a permitir uma maior personalização das mensagens enviadas pela sua empresa, bem como a análise do comportamento de compra feita automaticamente pelos nossos algoritmos de inteligência artificial.

Esses dados gerais de cadastro e clique serão usados para otimizar as campanhas feitas através da nossa plataforma e estarão sempre à sua disposição, podendo ser extraídos a qualquer momento, bem como integrados ao seu software de CRM.

Ao usuário do site do cliente também fica registrado o direito de se descadastrar da base a qualquer momento.

SOBRE O USO DOS DADOS PESSOAIS DE VISITANTES E CLIENTES

Os dados pessoais de clientes e visitantes serão usados apenas para eventuais cobranças de serviços, comunicados internos e envio de materiais educativos ou gerar pesquisas de mercado. Lembrando que jamais citaremos por escrito o nome da marca ou de seus respectivos funcionários sem autorização prévia.

SOBRE O USO DOS DADOS COLETADOS DE USUÁRIOS

Os dados pessoais coletados dos usuários serão usados e processados de forma automatizada pelos nossos algoritmos para entender padrões de comportamento e criar audiências segmentadas para as suas campanhas feitas pela nossa plataforma. Esses dados também serão usados em eventuais estudos de mercado e comportamento do consumidor, sendo que, nesses casos, tais dados terão as informações pessoais dos usuários deletadas, não se configurando mais um dado pessoal, e sim um mero conjunto de dados anônimos para fins de estudo e pesquisa.

Podemos utilizar automatização no processamento de dados para analisar as movimentações do usuário ou visitantes dentro do website, identificando conteúdos e produtos de interesse e, com base nisso, sugerir produtos de forma personalizada às preferências individuais.

SOBRE O ACESSO ÀS INFORMAÇÕES PESSOAIS DOS VISITANTES

O acesso aos dados pessoais dos visitantes é restrito aos funcionários da Social Miner - mais especificamente, às áreas de vendas, financeiro e marketing. Nenhuma informação pessoal poderá ser divulgada publicamente.

A Social Miner também se compromete a não vender, alugar ou repassar suas informações para terceiros. A única exceção está em casos em que essas informações forem exigidas judicialmente, comprometendo-se a Social Miner a restringir eventual exposição apenas ao que lhe for solicitado em juízo.

A Social Miner opera com os mais altos padrões de segurança de dados, mas não se responsabiliza por eventuais roubos de dados e invasões terceiras. Para mais informações, consulte o campo “Como protegemos suas informações?” abaixo.

SOBRE O ACESSO AOS DADOS DOS USUÁRIOS

O acesso aos dados dos usuários é restrito aos funcionários da Social Miner - mais especificamente, às áreas de engenharia, produto, customer success e marketing.

Fornecemos ao cliente dados gerais de resultado em sua plataforma, ou seja, de cadastro e clique, possibilitando, por meio de nossa plataforma, que o cliente individualize suas campanhas com base no comportamento dos usuários sem, contudo, possibilitar ao cliente o acesso ao comportamento individualizado de um usuário diretamente na plataforma.

Nenhuma informação pessoal dos usuários poderá ser divulgada publicamente. A única exceção está em casos de estudo de mercado, em que essas informações serão anonimizadas, não se configurando mais um dado pessoal relevante, sem jamais citar ou vincular marcas sem autorização prévia.

A Social Miner também se compromete a não vender, alugar ou repassar informações da base de usuário de clientes para terceiros. A única exceção está em casos em que essas informações forem exigidas judicialmente, comprometendo-se a Social Miner a restringir eventual exposição apenas ao que lhe for solicitado em juízo.

SOBRE O COMPARTILHAMENTO DE INFORMAÇÕES COM TERCEIROS

O acesso aos dados de usuários por terceiros é proibido pela Social Miner. Envidamos todos nossos esforços, por meio contratuais, para coibir esse tipo de prática, conhecida como Cookiepool pois, com base nas leis internacionais de proteção de dados e no Marco Civil da Internet, entendemos que o usuário só pode ter seu dado compartilhado com prévio consentimento.

Além da própria Social Miner, nenhuma outra empresa ou cliente terá acesso aos dados e informações pessoais dos seus leads. Somos contra a política de Cookiepool e jamais compartilharemos base entre os nossos clientes, uma vez que tais práticas constituem uma violação de privacidade do usuário e são nocivas ao mercado.

A Social Miner, no entanto, poderá compartilhar suas informações se assim for requerido por autoridade governamental, regulatória ou por decisão judicial, limitando-se a restringir tais dados apenas aos que nos for solicitado.

SOBRE O CANCELAMENTO DA ASSINATURA, ALTERAÇÃO OU EXCLUSÃO DE INFORMAÇÕES PESSOAIS

Você pode optar por não receber mais qualquer tipo de e-mail ou comunicado interno da Social Miner. Sempre oferecemos essa opção em quaisquer comunicações que você receber, dando-lhe a opção de cancelar a assinatura ou excluir seu nome da nossa base de cadastro, com base nos princípios das leis internacionais que regem o processamento de informações pessoais.

Para exercer o seu direito a objeção, basta clicar no link no rodapé do e-mail e você automaticamente será descadastrado da nossa lista.

Vale lembrar que, ao preencher qualquer formulário da Social Miner seus dados serão inseridos novamente na nossa lista de contato, necessitando um novo cancelamento de assinatura.

Para alterar suas informações pessoais ou mesmo excluí-las do nosso banco de dados, basta enviar um e-mail para privacy@socialminer.com. Caso você seja um usuário visitante de um cliente da Social Miner, recomendamos que entre em contato diretamente com o cliente, exercendo seus direitos de privacidade.

SOBRE A COLETA DE DADOS DE MENORES DE 13 ANOS

A Social Miner não coleta e nem mantém, conscientemente, dados pessoais de sujeitos com menos de 13 anos de idade. Recomendamos que se você como usuário ou visitante for menor de 13 anos, não navegue pelo nosso site ou de parceiros sem o acompanhamento de um responsável.

A Social Miner tomará todas as providências cabíveis para apagar quaisquer informações de dados pessoais coletadas sobre pessoas com menos de 13 anos de idade, quando feitas sem o consentimento confirmado dos pais, assim que for notificada acerca da existência de informações pessoalmente identificáveis.

POR QUANTO TEMPO A SOCIAL MINER MANTÉM AS INFORMAÇÕES?

Manteremos as informações processadas pelo período necessário para prover os serviços da nossa plataforma ou enquanto tivermos o seu consentimento para tanto.

Caso um usuário, visitante ou cliente nos contate solicitando exercer seu direito a objeção ou esquecimento, poderemos manter alguns dados para cumprir com obrigações legais.

Os dados do usuário com inatividade contínua por mais de 05 (cinco) anos terão suas ID's desvinculadas dos dados de comportamento, não configurando mais um dado pessoal relevante para fins legais, e sim um mero instrumento para estudos e pesquisas.

COMO PROTEGEMOS SUAS INFORMAÇÕES?

Todas as informações de dado pessoal que são processadas pela Social Miner são guardadas em servidores com altos padrões de segurança. Isso significa dizer que trazemos mais camadas de proteção às suas informações, tornando mais difícil a violação delas por terceiros.

Para mais informações, consulte: <https://aws.amazon.com/pt/compliance/programs/>

SOBRE OS FUNDAMENTOS JURÍDICOS PARA COLETA E PROCESSAMENTO DE DADOS DOS USUÁRIOS, VISITANTES E CLIENTES

A Social Miner só processará as informações pessoais de clientes, visitantes ou usuários quando tiver, nos moldes das legislações internacionais de proteção de dados, uma base legal por detrás. As bases legais podem variar, sendo, em suma:

- Por motivo de necessidade de uso de informação para provimento de produtos ou serviços de acordo com as preferências do usuário, conforme definido pelo nosso algoritmo de inteligência artificial, com base no comportamento do usuário dentro dos sites.
- Por termos interesse legítimo em usar os dados pessoais para operar e melhorar nossos serviços, sendo que, em caso de pesquisas e estudos, tais dados serão analisados de forma anônima, desvinculando-os de um usuário específico.
- Por haver consentimento entre os visitantes, usuário ou cliente, com relação ao uso de seus dados pessoais para um fim particular.

- Por necessitarmos utilizar os dados para execução contratual ou cumprir com quaisquer obrigações legais.

Caso o processamento dos dados seja feito com base em outras leis, a base para processamento pode não estar listada acima e pode, nestas circunstâncias, ser fundamentada no consentimento do visitante, usuário ou cliente para todos os fins.

MUDANÇAS NA POLÍTICA DE PRIVACIDADE

Essa Política de Privacidade pode passar por atualizações caso necessário. Por isso, recomendamos que visite periodicamente esta página para que você tenha conhecimento sobre as modificações.

Contudo, antes de modificar ou acrescentar pontos que não correspondam com esta Política de Privacidade, solicitaremos sua autorização via plataforma Social Miner.

ANEXO IV. POLÍTICA DE COOKIES - SOCIAL MINER

Buscando aprimorar ainda mais a transparência de nossos serviços com os visitantes, usuários e clientes, apresentamos nossa política de Cookies, que ensina o que são cookies, de qual forma os utilizamos no website/tecnologia, e suas escolhas de cookies em sua navegação.

A Política de Cookies deve ser lida juntamente com a Política de Privacidade, por se tratarem de instrumentos complementares.

O QUE SÃO COOKIES?

Cookies são definidos como pequenos arquivos de texto inserido no código do website da Social Miner e dos clientes que utilizam a tecnologia Social Miner. Sua principal função, ao ser armazenado em um navegador web é possibilitar que reconheçamos você e tornemos sua visita personalizada de acordo com suas preferências analisadas pela tecnologia Social Miner.

Em suma, visualizamos os cookies como cartões de identificação dos visitantes e usuários para a tecnologia Social Miner.

A Social Miner, com seu website e tecnologia, trabalha com cookies “persistentes” e de “sessão”. Por Cookies “persistentes”, entende-se todos aqueles que independentemente da navegação, sempre se mantêm registrados no servidor da Social Miner. Quando falamos de Cookies de “sessão”, referimo-nos aos comportamentos navegacionais dentro de uma janela única de navegação do usuário. Tais cookies se subdividem em:

Cookie analítico – São cookies que possibilitam o reconhecimento e contagem do número de visitantes, no intuito de demonstrar como se movem dentro do website e tecnologia. Nosso foco é melhorar a análise do comportamento do visitante/usuário.

Cookies de customização – Utilizamos tais cookies visando reconhecer o seu retorno ao website e tecnologia. Com isso, conseguimos tornar os conteúdos cada vez mais relevantes para os visitantes e usuários, enviar mensagens padronizadas e resgatar suas preferências.

Cookie de rastreamento – Esses cookies tem como função o registro da sua visita ao website ou tecnologia, quais páginas foram frequentadas e demais informações relevantes de navegação. Assim como os cookies de customização, nosso objetivo é tornar o site/tecnologia mais personalizado, com base em seus interesses.

Buscando aprimorar ainda mais a transparência de nossos serviços com os visitantes, usuários e clientes, apresentamos nossa política de Cookies, que ensina o que são cookies, de qual forma os utilizamos no website/tecnologia, e suas escolhas de cookies em sua navegação.

A Política de Cookies deve ser lida juntamente com a Política de Privacidade, por se tratarem de instrumentos complementares.

COMO GERENCIAR SUAS PREFERÊNCIAS DE COOKIE?

Os atuais navegadores de web possuem ferramentas que possibilitam o gerenciamento de suas preferências. Dentro do seu navegador, na aba de configurações, há a opção para recusar cookies ou excluí-los, de acordo com sua vontade.

Todavia, se você optar por bloquear os cookies durante a navegação em nosso website ou websites de clientes que utilizam nossa tecnologia, poderá comprometer a experiência de navegação personalizada de conteúdo proporcionada pela Social Miner.

ANEXO V. POLÍTICA DE PRIVACIDADE - MAGAZINE LUIZA

Este documento, denominado Política de Privacidade, possui finalidade de estabelecer as regras sobre o uso, armazenamento e tratamento dos dados e informações coletadas dos usuários no site magazineluiza.com.

1. Definições: para fins desta Política de Privacidade, aplicam-se as seguintes definições: designa o site magazineluiza.com. Magazine Luiza: Magazine Luiza S/A, pessoa jurídica de direito privado, com sede à Rua Voluntários da Franca, 1465 – Centro – Franca – SP, CEP 14400-490 e inscrita no CNPJ sob o nº 47.960.950/0001-21. Cookies: arquivos enviados pelo servidor do site para o computador do Usuário, com a finalidade de identificar o computador e obter dados de acesso, como páginas navegadas ou links clicados, permitindo, desta forma, personalizar a utilização do site, de acordo com o seu perfil; IP: abreviatura de Internet Protocol. É um conjunto de números que identifica o computador do Usuário na Internet; Logs: registros de atividades do Usuário efetuadas no site; Session ID: identificação da sessão do Usuário no processo de inscrição ou quando utilizado de alguma forma o site. Usuário: todo aquele que passar a usar o site.

2. Obtenção dos dados e informações: os dados e informações serão obtidos quando o Usuário: 1. Passar a utilizar o site; 2. Interagir com as diversas ferramentas existentes no site, fornecendo as informações voluntariamente; ou 3. Entrar em contato através dos canais de comunicação disponíveis no site.

3. Armazenamento dos Dados e Informações: todos os dados e informações coletados dos Usuários serão incorporados ao banco de dados do site, sendo seu responsável e proprietário o Magazine Luiza. Os dados e informações coletados estarão armazenados em ambiente seguro, observado o estado da técnica disponível, e somente poderão ser acessados por pessoas qualificadas e autorizadas pelo Magazine Luiza. Além disso, o Magazine Luiza afirma que não compartilhará, venderá ou apresentará os dados dos Usuários para terceiros. Considerando que nenhum sistema de segurança é absolutamente seguro, o Magazine Luiza se exime de quaisquer responsabilidades por eventuais danos e/ou prejuízos decorrentes de falhas, vírus ou invasões do banco de dados do site, salvo nos casos de dolo ou culpa pela mesma. O Usuário é o proprietário dos dados e está apto a adicionar, excluir ou modificar quaisquer informações que estiverem ligadas ao seu perfil de usuário no Magazine Luiza.

4. Uso dos Dados e Informações: os dados e informações coletados dos Usuários poderão ser utilizados para as seguintes finalidades: 1. Efetuar qualquer comunicação resultante de atividade do próprio site ou a identificação do respectivo destinatário; 2. Responder a eventuais dúvidas e solicitações do Usuário; 3. Fornecer acesso à área restrita do site ou suas funcionalidades exclusivas; 4. Cumprimento de ordem legal ou judicial; 5. Constituir, defender ou exercer regularmente

direitos em âmbito judicial ou administrativo; 6. Elaborar estatísticas gerais, para identificação do perfil dos Usuários e desenvolvimento de campanhas do Magazine Luiza; 7. Garantir a segurança dos Usuários; 8. Manter atualizados os cadastros dos Usuários para fins de contato autorizado a ser feito por telefone, correio eletrônico, SMS, mala-direta ou por outros meios de comunicação; 9. Informar a respeito de novidades, promoções e eventos do Magazine Luiza e seus parceiros comerciais.

4.1. Sobre os e-mails: serão enviados e-mails diariamente com ofertas para os clientes cadastrados. Os e-mails enviados pelo Magazine Luiza não contêm anexos para serem baixados e tampouco solicitam dados dos usuários.

4.2. Caso o Cliente não queira mais receber e-mails do Magazine Luiza, ele deve clicar no link de descadastramento presente em todos os e-mails enviados.

5. Do Registro de Atividades: o Magazine Luiza poderá registrar as atividades efetuadas pelo Usuário no site, por meio de logs, incluindo: 1. Endereço IP do Usuário; 2. Ações efetuadas pelo Usuário no site; 3. Páginas acessadas pelo Usuário; 4. Datas e horários de cada ação e de acesso a cada funcionalidade do site; 5. Session ID do Usuário, quando aplicável. Os registros mencionados poderão ser utilizados pelo Magazine Luiza em casos de investigação de fraudes ou de alterações indevidas em seus sistemas e cadastros.

6. Cookies: o site poderá fazer o uso de cookies, cabendo ao Usuário configurar o seu navegador de Internet, caso deseje bloqueá-los. Nesta hipótese, algumas funcionalidades do site poderão ser limitadas.

7. Recomendações: a partir do uso de um cookie que identifica a navegação do Usuário, o site faz a recomendação de produtos. Essa recomendação varia conforme o Usuário e seu comportamento dentro do site, sendo avaliado, por exemplo, se houve apenas navegação ou também compra, quais itens foram vistos, pesquisados ou comprados por ele e outros Usuários em situações de navegação semelhantes. Considerando que essa recomendação é gerada a partir de algoritmos, sua precisão pode não ser exata, porém visa sugerir produtos que sejam do interesse do Usuário, sem que este tenha qualquer obrigatoriedade de adquiri-los.

8. Disposições Gerais: as disposições constantes desta Política de Privacidade poderão ser atualizadas ou modificadas a qualquer momento, cabendo ao Usuário verificá-la sempre que efetuar o acesso ao site. O Usuário deverá entrar em contato em caso de qualquer dúvida com relação às disposições constantes desta Política de Privacidade e Uso, elegendo um destes meios de contato: telefone 0800-34-4000 ou formulário de contato.

9. Lei Aplicável e Jurisdição: a presente Política de Privacidade será interpretada segundo a legislação brasileira, no idioma

português, sendo eleito o Foro da Comarca de São Paulo para dirimir qualquer litígio, questão ou dúvida superveniente, com expressa renúncia de qualquer outro, por mais privilegiado que seja.

10. Cadastro: para participar e usufruir do site, além de ter a idade mínima de 18 (dezoito) anos, o Cliente deverá fornecer na ocasião do cadastro as seguintes informações: nome completo, apelido, CPF, RG, endereço completo, telefone fixo, data de nascimento, e-mail, além de escolher uma senha.

11. A regra de desconto varia de acordo com a categoria. Categorias com 5% de desconto: Móveis, Colchões, Utensílios Domésticos, Relógios, Esporte e Lazer, Ferramentas e Segurança, Perfumaria Categorias com 10% de desconto: Informática e Acessórios, Ar Condicionado, Eletrodomésticos, Eletroportáteis, Beleza e Saúde, Bebês, Brinquedos, Casa e Jardim, Tablets, Telefonia Fixa, Celulares e Telefonia, TV e Video, Games, Áudio e Auto

Atualização: 23 de Julho de 2015.

ANEXO VI. TERMOS DE USO DO AMAZON PRIME VIDEO

Última atualização: 6 de fevereiro de 2019

Bem-vindo aos termos de uso do Amazon Prime Video. Estes termos são válidos entre você e a empresa que lhe fornece o serviço Amazon Prime Video, a qual poderá ser, conforme sua localização, Amazon Digital Services LLC, Amazon Video Limited ou uma de suas afiliadas (“Amazon” ou “nós”). Acesse www.primevideo.com/ww-av-legal-home para identificar a afiliada Amazon responsável por seu serviço Amazon Prime Video e consulte outros termos aplicáveis com base em sua localização. O fornecedor do serviço Amazon Prime Video poderá mudar de tempos em tempos, com ou sem notificação prévia (salvo se exigido por lei). Por favor, leia estes termos, assim como o Aviso de Privacidade, as Condições de Uso e as Regras de Uso Amazon Prime Video aplicáveis a você), e quaisquer outras regras e políticas relacionadas ao serviço Amazon Prime Video (inclusive, mas não apenas, quaisquer regras ou determinações de uso especificadas em qualquer página de informações detalhadas do produto, ou qualquer página de ajuda ou outra página informativa do serviço Amazon Prime Video) (no conjunto, este “Contrato”). Se você está localizado na União Europeia, o Aviso de Privacidade, as Condições de Uso, o Aviso de Cookies e o Aviso de Anúncios Baseados em Interesses não fazem parte do seu contrato. As versões destas políticas e notificações aplicáveis a você estão disponíveis para sua análise para entender como lidamos com sua informação pessoal. Toda vez que você acessar, navegar ou utilizar o serviço Amazon Prime Video, você estará automaticamente de acordo com os termos deste Contrato.

1. SERVIÇO

Amazon Prime Video (o “Serviço”) é um serviço personalizado que oferece, recomenda e ajuda a descobrir filmes digitais, programas de TV e outros conteúdos de vídeo (conjuntamente, “Conteúdo Digital”) e outros serviços, conforme previsto neste Contrato. O Serviço e o Conteúdo Digital podem ser acessados de várias formas, inclusive por meio do Amazon Prime, e o seu uso de outros benefícios do Prime e serviços Amazon é regido por termos disponibilizados a você nos aplicativos, sites e dispositivos que você utiliza para acessar tais serviços. Se você tem menos de 18 anos, ou é menor de idade segundo a regra de sua localidade, você poderá utilizar o Serviço apenas mediante a participação de pai, mãe ou responsável. Personalizamos o conteúdo e os recursos como parte dos Serviços, inclusive mostrando-lhe recomendações sobre o conteúdo digital, recursos e serviços que podem lhe interessar. Também nos esforçamos para melhorar continuamente os dispositivos e serviços da Amazon e sua experiência com eles.

2. DISPOSITIVOS COMPATÍVEIS

Para acessar Conteúdo Digital, seja via streaming ou download, você precisará de um computador pessoal, reproduzidor de mídia portátil ou outro dispositivo que atende os requisitos de sistema e compatibilidade estabelecidos por nós de tempos em tempos (um “Dispositivo Compatível”). Alguns Dispositivos Compatíveis poderão ser utilizados apenas para acessar o Conteúdo Digital via streaming, alguns poderão ser utilizados apenas para baixar (download) Conteúdo Digital, e alguns poderão ser utilizados tanto para baixar quanto para acessar por streaming o Conteúdo Digital. Nós poderemos mudar os pré-requisitos dos Dispositivos Compatíveis de tempos em tempos e, em alguns casos, a manutenção ou exclusão de um dispositivo na lista de Dispositivos Compatíveis poderá depender de softwares ou sistemas fornecidos ou mantidos pelo fabricante do dispositivo ou terceiros. Assim, dispositivos indicados como Dispositivos Compatíveis em um determinado momento podem deixar de ser Dispositivos Compatíveis no futuro. A entidade legal da Amazon que lhe fornece o aplicativo de celular do Amazon Prime Video pode não ser a mesma entidade legal da Amazon que fornece o Serviço.

3. VARIABILIDADE GEOGRÁFICA

Devido a restrições técnicas e outras limitações impostas por fornecedores de conteúdo, o Serviço estará disponível apenas em certas localidades. O Conteúdo Digital (incluindo versões dubladas e legendadas do Conteúdo Digital) e o modo como o oferecemos a você deverá variar conforme o tempo e a localidade. A Amazon utilizará tecnologias para verificar a sua localização geográfica. Você não poderá utilizar qualquer técnica ou tecnologia para confundir ou ocultar a sua localização.

4. CONTEÚDO DIGITAL

a. Geral. O Serviço permitirá a você: (i) acessar o Conteúdo Digital através de uma assinatura, por tempo limitado, durante o período da assinatura (por exemplo, por meio do Amazon Prime, ou outra oferta de vídeo, autônoma ou por assinatura) (“Conteúdo Digital por Assinatura”), (ii) alugar Conteúdo Digital para assistir sob demanda por um tempo limitado (“Conteúdo Digital Alugado”), (iii) comprar Conteúdo Digital para assistir sob demanda por tempo ilimitado (“Conteúdo Digital Comprado”), (iv) comprar Conteúdo Digital para assistir no sistema pay-per-view por um tempo limitado (“Conteúdo Digital PPV”), e/ou (v) acessar Conteúdo Digital gratuitamente, mantido via publicidade ou por meio de promoção para assistir por tempo limitado (“Conteúdo Digital Gratuito”). O Conteúdo Digital poderá estar disponível como Conteúdo Digital por Assinatura, Conteúdo Digital Alugado, Conteúdo Digital Comprado, Conteúdo Digital PPV, Conteúdo Digital Gratuito, ou qualquer combinação dessas categorias, sujeito, em cada caso, à licença de natureza limitada concedida abaixo.

b. Regras de Uso. A utilização do Conteúdo Digital estará sujeita às Regras de Uso do Amazon Prime Video (“Regras de

Uso”). As Regras de Uso fornecem informações importantes, incluindo o período de tempo durante o qual você estará autorizado a assistir os diversos tipos de Conteúdo Digital (o “Período de Acesso”) e limitações quanto ao número e o tipo dos Dispositivos Compatíveis pelos quais o Conteúdo Digital poderá ser transmitido, baixado e assistido.

c. Assinaturas/Adesão a Programas. Condições de preço e ofertas para assinaturas (também referido aqui como adesões a programas), serviços de assinatura, a extensão do Conteúdo Digital por Assinatura disponível e os títulos específicos disponíveis pelos serviços de assinatura poderão mudar conforme o tempo e a localização, sem aviso (salvo se exigido por lei). A menos que indicado de outra forma, quaisquer alterações de preço são efetivas a partir do início do próximo período de assinatura. Se você não estiver de acordo com uma modificação na assinatura, você poderá cancelar a assinatura de acordo com os termos da Seção 4(d) abaixo. Os preços para assinatura ou adesão a programas podem incluir VAT ou outros tributos. Quando aplicável, tais tributos serão recolhidos pela parte que recebe o pagamento pela sua assinatura ou adesão a programa, que poderá ser a Amazon ou um terceiro. Não oferecemos garantias quanto à disponibilidade de um Conteúdo Digital por Assinatura específico ou quanto a uma quantidade mínima de Conteúdo Digital por Assinatura disponível em determinada categoria de assinatura. Termos adicionais válidos para a assinatura (como a política de cancelamento e reembolso aplicável) serão indicados nas páginas de informação da respectiva assinatura no website principal do Serviço, para sua localidade, disponíveis aqui (seu “Video Marketplace”).

Alguns dos serviços de assinatura que oferecemos provêm de terceiros. Terceiros responsáveis por fornecer serviços de assinatura (por exemplo, por meio dos Canais Prime Video) poderão modificar ou interromper as ferramentas de seus serviços ou o conteúdo de seus serviços. A Amazon não é responsável pelo conteúdo disponível em serviços de assinaturas de terceiros ou pelas ferramentas daqueles serviços.

d. Cancelamento de Assinatura/Adesão a Programa. Você poderá cancelar uma assinatura de apenas vídeo ou adesão a um programa a qualquer momento, ajustando suas opções de assinatura/filiação na Sua Conta, entrando em contato com o serviço de atendimento ao consumidor da Amazon, ou preenchendo qualquer formulário de cancelamento disponível no seu Video Marketplace (disponível aqui), ou caso você pague pela Amazon assinatura ou adesão a programa por meio de um terceiro, através da sua conta com tal terceiro. Em caso de cancelamento antes de transcorridos 3 dias úteis da assinatura ou da conversão de um período experimental gratuito em assinatura paga (ou, para clientes na União Europeia, antes de 14 dias da confirmação da sua assinatura ou filiação), você será integralmente reembolsado do valor da assinatura; contudo, você poderá ser cobrado (ou ter descontado de seu reembolso) o valor do Serviço utilizado através da sua conta no período. Você também concorda expressamente que o Serviço começará dentro do período de cancelamento. Em caso de cancelamento em qualquer outro momento, você será reembolsado integralmente do valor da assinatura somente se

o Conteúdo Digital disponível como parte da assinatura de apenas vídeo não tiver sido acessado por meio de sua conta depois da última cobrança da sua assinatura. Se você acessar o Serviço como membro Prime, os termos de cancelamento e reembolso aplicáveis estão definidos nos Termos de Uso Prime do seu Video Marketplace (disponível aqui). Caso você pague pela assinatura ou adesão a programa por meio de um terceiro, os termos do cancelamento e reembolso aplicáveis a você podem ser distintos e são estabelecidos por tal terceiro.

e. Operações de Compra e Locação; Cancelamentos. Exceto conforme descrito neste parágrafo, todas as operações de Conteúdo Digital Comprado, Conteúdo Digital Alugado e Conteúdo Digital PPV são definitivas, e não é admitida a devolução de tais Conteúdos Digitais.

Você poderá cancelar um pedido de Conteúdo Digital Comprado ou Conteúdo Digital Alugado até 48 horas após a compra ou locação (ou, para clientes na União Europeia, dentro de 14 dias da data de compra ou locação) clicando em “Cancele seu Pedido”, em Seus Pedidos Digitais no Video Marketplace (indicado aqui) ou entrando em contato com o serviço de atendimento da Amazon; contudo, você não poderá cancelar um pedido de Conteúdo Digital Comprado ou Conteúdo Digital Alugado após começar a assistir ou baixar tais Conteúdos Digitais. Você poderá cancelar um pedido de pré-venda de Conteúdo Digital Comprado ou Conteúdo Digital Alugado a qualquer momento antes da data de lançamento. Você poderá cancelar um pedido de Conteúdo Digital PPV a qualquer momento antes do início programado do programa. A data de lançamento de um Conteúdo Digital disponível para pré-venda poderá ser mudada.

f. Métodos de Pagamento. Se não for possível processar o seu pagamento pelo método de pagamento indicado por você, nos reservamos o direito de fazer a cobrança por qualquer outro método de pagamento que conste em nossos registros. Se você comprar uma assinatura ou iniciar um período gratuito de assinatura, sua assinatura continuará automaticamente, e você nos autoriza (sem outro aviso, exceto se exigido por lei) a cobrar o valor periódico da assinatura então aplicável, incluídos os tributos, utilizando qualquer método de pagamento que conste em nossos registros. Continuaremos cobrando a respectiva assinatura até que ela seja cancelada. Se todos os seus métodos de pagamento em nossos registros forem recusados para o pagamento do valor da assinatura, sua assinatura será cancelada, a menos que você indique um novo método de pagamento. Se você informar um novo método de pagamento e o valor da assinatura for cobrado com sucesso antes da assinatura ser cancelada, o seu novo período de assinatura será baseado na data de vencimento original e não na data da cobrança bem-sucedida. Você pode utilizar as opções na “Sua Conta” para atualizar seus métodos de pagamento.

g. Acesso Promocional. Assinaturas gratuitas ou outras modalidades promocionais de assinatura podem ser oferecidas a certos clientes; elas estarão sujeitas a este Contrato, exceto se determinado de outro modo nos termos da oferta promocional. A elegibilidade dos clientes para desfrutar de qualquer promoção fica a critério exclusivo da Amazon. Assinantes em

período de teste poderão a qualquer tempo (por meio da Sua Conta) decidir não manter a assinatura paga ao final do período experimental.

h. Licença Limitada ao Conteúdo Digital. Sujeito ao pagamento de valores para alugar, comprar ou acessar Conteúdo Digital, e ao adimplemento de todos os termos deste Contrato, a Amazon concede a você uma licença limitada, não exclusiva, não transferível, não sublicenciável, durante o Período de Acesso aplicável, para acessar e visualizar o Conteúdo Digital em conformidade com as Regras de Uso, para uso pessoal, não comercial e privado. Nós poderemos remover automaticamente o Conteúdo Digital do seu Dispositivo Compatível após o término do Período de Acesso.

i. Disponibilidade do Conteúdo Digital Comprado. O Conteúdo Digital Comprado geralmente continuará disponível para download ou streaming a partir do Serviço, conforme o caso, mas poderá tornar-se indisponível devido a potenciais restrições de licenciamento do provedor de conteúdo ou por outros motivos, e a Amazon não será responsável perante você se o Conteúdo Digital Comprado tornar-se indisponível para futuro download ou streaming.

j. Qualidade de Reprodução; Streaming. A qualidade e resolução de reprodução do Conteúdo Digital que você recebe dependerá de um número de fatores, incluindo o tipo de Dispositivo Compatível no qual você está acessando o Conteúdo Digital e a velocidade da sua conexão, que poderá aumentar ou diminuir durante a visualização. Se detectarmos que o Conteúdo Digital que estamos disponibilizando a você via streaming poderá ser interrompido, ou de outra forma poderá ter sua reprodução afetada por limitações de conexão ou outros fatores, poderemos diminuir a resolução e o tamanho do arquivo do Conteúdo Digital oferecido por streaming como forma de fornecer uma experiência contínua de visualização. Mesmo fazendo o máximo esforço para fornecer uma experiência de alta qualidade de visualização, não oferecemos garantias quanto à resolução ou qualidade do Conteúdo Digital ao qual você terá acesso por streaming, mesmo que tenha pagado um valor extra para ter conteúdo de alta definição (HD), de ultra-alta definição (UHD) ou de grande alcance dinâmico (HDR).

k. Restrições Gerais. Você não poderá (i) transferir, copiar ou exibir o Conteúdo Digital, salvo nos termos autorizados por este Contrato; (ii) vender, alugar, conceder, distribuir ou transmitir qualquer direito ao Conteúdo Digital; (iii) remover qualquer aviso de propriedade intelectual ou etiqueta do Conteúdo Digital; (iv) tentar desabilitar, evitar, modificar, frustrar ou de outra forma contornar qualquer método de gestão de direito digital ou outro sistema de proteção de conteúdo utilizado como parte do Serviço; ou (v) utilizar o Serviço ou Conteúdo Digital para qualquer propósito comercial ou ilegal.

l. Medição de Audiência. Para clientes nos EUA determinados terceiros, como anunciantes e proprietários de conteúdo, se interessam em entender a performance do conteúdo de tais terceiros nos Canais Prime Video. Ao visualizar certos Canais, a Amazon poderá fornecer a terceiros informações sobre o seu comportamento de visualização para fins de medição de

audiência e pesquisa de mercado. Clique aqui para mais informações sobre esses serviços de medição, Canais que os possuem e suas escolhas.

5. SOFTWARE

a. Utilização do Software. Nós poderemos disponibilizar software para uso relacionado ao Serviço (“Software”). Os termos contidos nas Condições de Uso do seu Video Marketplace (indicados aqui) aplicam-se ao uso do Software. Para termos adicionais que se aplicam a certos Softwares de terceiros, clique aqui.

b. Informações Fornecidas à Amazon. O Serviço e o Software poderão fornecer à Amazon informações relativas ao seu uso e à performance do Serviço e do Software, assim como informações referentes aos dispositivos nos quais você baixa e utiliza o Serviço e o Software. Por exemplo, o Software poderá fornecer à Amazon informações relativas ao Conteúdo Digital que você baixa ou acessa via streaming e o seu uso desse Conteúdo Digital (como, por exemplo, se você visualizou um Conteúdo Digital e quando fez isso, o que poderá, entre outras coisas, nos ajudar a medir o Período de Acesso para Conteúdo Digital Alugado). Qualquer informação que recebermos estará sujeita ao Aviso de Privacidade da Amazon no seu Video Marketplace (indicado aqui).

6. TERMOS ADICIONAIS

a. Rescisão. Nós poderemos rescindir o acesso ao Serviço, inclusive qualquer assinatura disponível como parte do Serviço, a nosso critério, sem aviso (salvo se exigido por lei). Se assim fizermos, daremos a você um reembolso proporcional do valor da assinatura (se for o caso); entretanto, se você infringir qualquer dos termos deste Contrato, os seus direitos nos termos deste Contrato serão automaticamente extintos, sem aviso, e a Amazon poderá, discricionariamente, revogar de imediato o seu acesso ao Serviço e ao Conteúdo Digital, sem restituir qualquer valor. Nesse caso, você deverá deletar todas as cópias do Conteúdo Digital de que tiver feito download.

b. Conteúdo Explícito. Ao usar o Serviço, você poderá encontrar conteúdo potencialmente ofensivo, indecente ou questionável; esse conteúdo poderá ou não ser identificado como tendo linguagem explícita ou outros atributos. Entretanto, você concorda em utilizar o Serviço sob seu próprio e exclusivo risco e a Amazon não tem responsabilidade perante você por qualquer conteúdo. Tipos de conteúdo, gêneros, categorias e descrições são fornecidos a título de conveniência, e a Amazon não garante a sua exatidão.

c. Comunicações. Nós poderemos lhe enviar promoções ou manter a comunicação com você por via eletrônica o que pode-

rá incluir e-mail, notificações por push, ou postagens no seu Centro de Mensagens Amazon, e você consente por meio deste em receber essas mensagens (a menos que você seja um cliente na União Europeia, caso em que a frase anterior não se aplica). Essas mensagens estarão de acordo com o Aviso de Privacidade da Amazon no seu Video Marketplace (indicado aqui). Para deixar de receber comunicações de marketing do Amazon Prime Video, atualize suas preferências de comunicação de marketing na Sua Conta.

d. Mudança do Serviço. A Amazon reserva o direito de modificar, suspender ou interromper o Serviço, ou qualquer parcela do Serviço, a qualquer tempo e sem aviso (salvo nos termos da legislação aplicável), e a Amazon não será responsabilizada por exercer tais direitos, mesmo que a sua capacidade de uso do Conteúdo Digital seja afetada pela mudança.

e. Alterações. A Amazon reserva o direito de fazer alterações neste Contrato a qualquer tempo, postando os termos revisados relativos ao Serviço ou no seu Video Marketplace (indicado aqui). No limite máximo admitido pela lei, a continuidade do seu uso do Serviço ou do Software após quaisquer alterações implicará a aceitação de tais alterações. Entretanto, qualquer aumento no valor da assinatura não será aplicado antes da renovação da sua assinatura.

f. Reserva de Direitos; Renúncia. O Serviço, o Software e o Conteúdo Digital contêm propriedade intelectual protegida por lei. Detentores de Direitos Autorais de Conteúdo Digital são tidos como terceiros beneficiários nos termos do Contrato. O fato de não exigirmos judicialmente a execução específica do Contrato não constituirá uma renúncia de qualquer dos nossos direitos.

g. Controvérsias/Condições de Uso. Qualquer controvérsia ou ação decorrente ou relacionada a este Contrato ou ao Serviço estará sujeita a lei regente, exclusão de garantias e limitação de responsabilidade e todos os demais termos nas Condições de Uso da Amazon em seu Video Marketplace (indicado aqui). Você está de acordo com esses termos ao utilizar o Serviço. VOCÊ TAMBÉM PODERÁ DISPOR DE DIREITOS DECORRENTES DA LEGISLAÇÃO DE DIREITOS DO CONSUMIDOR NO MBITO DA SUA JURISDIÇÃO LOCAL.

h. Limitação de Responsabilidade. Sem limitar a exclusão de garantias e limitação de responsabilidade nas Condições de Uso da Amazon de seu Video Marketplace (indicado aqui): (i) em nenhuma hipótese a nossa responsabilidade total ou a dos licenciadores de nosso software perante a você por todos os danos decorrentes ou relacionados ao seu uso ou inabilidade de uso do Software excederá o valor de cinquenta dólares (US\$50); e (ii) em nenhuma hipótese nossa responsabilidade total ou a de nosso provedor de Conteúdo Digital decorrente do uso dos Serviços, do Conteúdo Digital, ou de informação, materiais ou produtos incluídos ou de outro modo disponibilizados a você por meio do Serviço excederá o valor que você tiver pago a nós nos 12 meses anteriores pela compra, locação ou visualização do Conteúdo Digital referente à

sua reclamação de danos. As limitações nesta seção serão aplicadas a você mesmo que as medidas judiciais não tenham êxito.

CERTAS JURISDIÇÕES, INCLUINDO JURISDIÇÕES NA UNIÃO EUROPEIA, NÃO PERMITEM A EXCLUSÃO DE GARANTIAS IMPLÍCITAS OU A LIMITAÇÃO OU EXCLUSÃO DE RESPONSABILIDADE PARA CERTOS TIPOS DE DANOS. SE ESSAS LEIS SE APLICAM A VOCÊ, PARTE DE OU TODAS AS ISENÇÕES, EXCLUSÕES OU LIMITAÇÕES DE RESPONSABILIDADE ACIMA PODEM NÃO SER APLICÁEIS A VOCÊ, E VOCÊ PODERÁ DISPOR DE DIREITOS ADICIONAIS.

i. Informações de Contato. Para comunicações relativas a este Contrato, por favor, escreva para a Amazon no endereço aplicável, indicado aqui.

j. Divisibilidade. Se qualquer termo ou condição deste Contrato for considerada inválida, nula ou ineficaz, essa parte será considerada separável e não afetará a validade e eficácia de qualquer termo ou condição remanescente.

ANEXO VII. AMAZON PRIVACY NOTICE

Last updated: August 29, 2017. To see what has changed, [click here](#).

Amazon.com knows that you care how information about you is used and shared, and we appreciate your trust that we will do so carefully and sensibly. This notice describes our privacy policy. By visiting Amazon.com, you are accepting the practices described in this Privacy Notice.

[What Personal Information About Customers Does Amazon.com Gather?](#)

[What About Cookies?](#)

[Does Amazon.com Share the Information It Receives?](#)

[How Secure Is Information About Me?](#)

[What About Third-Party Advertisers and Links to Other Websites?](#)

[Which Information Can I Access?](#)

[What Choices Do I Have?](#)

[Are Children Allowed to Use Amazon.com?](#)

[EU-US and Swiss-US Privacy Shield](#)

[Conditions of Use, Notices, and Revisions](#)

[Examples of Information Collected](#)

WHAT PERSONAL INFORMATION ABOUT CUSTOMERS DOES AMAZON.COM GATHER?

The information we learn from customers helps us personalize and continually improve your Amazon experience. Here are the types of information we gather.

Information You Give Us: We receive and store any information you enter on our Web site or give us in any other way. [Click here](#) to see examples of what we collect. You can choose not to provide certain information, but then you might not be able to take advantage of many of our features. We use the information that you provide for such purposes as responding to

your requests, customizing future shopping for you, improving our stores, and communicating with you.

Automatic Information: We receive and store certain types of information whenever you interact with us. For example, like many Web sites, we use “cookies,” and we obtain certain types of information when your Web browser accesses Amazon.com or advertisements and other content served by or on behalf of Amazon.com on other Web sites. [Click here](#) to see examples of the information we receive.

Mobile: When you download or use apps created by Amazon or our subsidiaries, we may receive information about your location and your mobile device, including a unique identifier for your device. We may use this information to provide you with location-based services, such as advertising, search results, and other personalized content. Most mobile devices allow you to turn off location services. For more information about how to do this, [click here](#) .

E-mail Communications: To help us make e-mails more useful and interesting, we often receive a confirmation when you open e-mail from Amazon.com if your computer supports such capabilities. We also compare our customer list to lists received from other companies, in an effort to avoid sending unnecessary messages to our customers. If you do not want to receive e-mail or other mail from us, please adjust your Customer Communication Preferences .

Information from Other Sources: We might receive information about you from other sources and add it to our account information. [Click here](#) to see examples of the information we receive.

WHAT ABOUT COOKIES?

Cookies are unique identifiers that we transfer to your device to enable our systems to recognize your device and to provide features such as 1-Click purchasing, Recommended for You , personalized advertisements on other Web sites (e.g., Amazon Associates with content served by Amazon.com and Web sites using Checkout by Amazon payment service), and storage of items in your Shopping Cart between visits.

The Help feature on most browsers will tell you how to prevent your browser from accepting new cookies, how to have the browser notify you when you receive a new cookie, or how to disable cookies altogether. Additionally, you can disable or delete similar data used by browser add-ons, such as Flash cookies, by changing the add-on’s settings or visiting the Web site of its manufacturer. Because cookies allow you to take advantage of some of Amazon.com’s essential features, we recommend that you leave them turned on. For instance, if you block or otherwise reject our cookies, you will not be able to add items to your Shopping Cart, proceed to Checkout, or use any Amazon.com products and services that require you to Sign in.

DOES AMAZON.COM SHARE THE INFORMATION IT RECEIVES?

Information about our customers is an important part of our business, and we are not in the business of selling it to others. We share customer information only as described below and with subsidiaries Amazon.com, Inc. controls that either are subject to this Privacy Notice or follow practices at least as protective as those described in this Privacy Notice.

Affiliated Businesses We Do Not Control: We work closely with affiliated businesses. In some cases, such as Marketplace sellers, these businesses operate stores at Amazon.com or sell offerings to you at Amazon.com. In other cases, we operate stores, provide services, or sell product lines jointly with these businesses. Click here for some examples of co-branded and joint offerings. You can tell when a third party is involved in your transactions, and we share customer information related to those transactions with that third party.

Third-Party Service Providers: We employ other companies and individuals to perform functions on our behalf. Examples include fulfilling orders, delivering packages, sending postal mail and e-mail, removing repetitive information from customer lists, analyzing data, providing marketing assistance, providing search results and links (including paid listings and links), processing credit card payments, and providing customer service. They have access to personal information needed to perform their functions, but may not use it for other purposes.

Promotional Offers: Sometimes we send offers to selected groups of Amazon.com customers on behalf of other businesses. When we do this, we do not give that business your name and address. If you do not want to receive such offers, please adjust your Customer Communication Preferences .

Business Transfers: As we continue to develop our business, we might sell or buy stores, subsidiaries, or business units. In such transactions, customer information generally is one of the transferred business assets but remains subject to the promises made in any pre-existing Privacy Notice (unless, of course, the customer consents otherwise). Also, in the unlikely event that Amazon.com, Inc., or substantially all of its assets are acquired, customer information will of course be one of the transferred assets.

Protection of Amazon.com and Others: We release account and other personal information when we believe release is appropriate to comply with the law; enforce or apply our Conditions of Use and other agreements; or protect the rights, property, or safety of Amazon.com, our users, or others. This includes exchanging information with other companies and organizations for fraud protection and credit risk reduction. Obviously, however, this does not include selling, renting, sharing, or otherwise disclosing personally identifiable information from customers for commercial purposes in violation of the commitments set forth in this Privacy Notice.

With Your Consent: Other than as set out above, you will receive notice when information about you might go to third parties, and you will have an opportunity to choose not to share the information.

HOW SECURE IS INFORMATION ABOUT ME?

We work to protect the security of your information during transmission by using Secure Sockets Layer (SSL) software, which encrypts information you input.

We reveal only the last four digits of your credit card numbers when confirming an order. Of course, we transmit the entire credit card number to the appropriate credit card company during order processing.

It is important for you to protect against unauthorized access to your password and to your computer. Be sure to sign off when finished using a shared computer. [Click here](#) for more information on how to sign off.

WHAT ABOUT THIRD-PARTY ADVERTISERS AND LINKS TO OTHER WEBSITES?

Our site includes third-party advertising and links to other Web sites. For more information about third-party advertising at Amazon.com, including personalized or interest-based ads, please read our [Interest-Based Ads policy](#).

WHICH INFORMATION CAN I ACCESS?

Amazon.com gives you access to a broad range of information about your account and your interactions with Amazon.com for the limited purpose of viewing and, in certain cases, updating that information. [Click here](#) to see some examples, the list of which will change as our Web site evolves.

WHAT CHOICES DO I HAVE?

As discussed above, you can always choose not to provide information, even though it might be needed to make a purchase or to take advantage of such Amazon.com features as Your Profile, Wish Lists , Customer Reviews, and Amazon Prime.

You can add or update certain information on pages such as those referenced in the Which Information Can I Access? section. When you update information, we usually keep a copy of the prior version for our records.

If you do not want to receive e-mail or other mail from us, please adjust your Customer Communication Preferences . (If you do not want to receive Conditions of Use and other legal notices from us, such as this Privacy Notice, those notices will still

govern your use of Amazon.com, and it is your responsibility to review them for changes.)

If you do not want us to use personal information that we gather to allow third parties to personalize advertisements we display to you, please adjust your Advertising Preferences .

The Help feature on most browsers will tell you how to prevent your browser from accepting new cookies, how to have the browser notify you when you receive a new cookie, or how to disable cookies altogether. Additionally, you can disable or delete similar data used by browser add-ons, such as Flash cookies, by changing the add-on's settings or visiting the Web site of its manufacturer. Because cookies allow you to take advantage of some of Amazon.com's essential features, we recommend that you leave them turned on. For instance, if you block or otherwise reject our cookies, you will not be able to add items to your Shopping Cart, proceed to Checkout, or use any Amazon.com products and services that require you to Sign in.

ARE CHILDREN ALLOWED TO USE AMAZON.COM?

Amazon.com does not sell products for purchase by children. We sell children's products for purchase by adults. If you are under 18, you may use Amazon.com only with the involvement of a parent or guardian. We do not knowingly collect personal information from children under the age of 13 without the consent of the child's parent or guardian. For more information, please see our Children's Privacy Disclosure.

EU-US AND SWISS-US PRIVACY SHIELD

Amazon.com, Inc. participates in the EU-US and Swiss-US Privacy Shield frameworks. [Click here to learn more.](#)

CONDITIONS OF USE, NOTICES, AND REVISIONS

If you choose to visit Amazon.com, your visit and any dispute over privacy is subject to this Notice and our Conditions of Use, including limitations on damages, resolution of disputes, and application of the law of the state of Washington. If you have any concern about privacy at Amazon.com, please contact us with a thorough description, and we will try to resolve it. Our business changes constantly, and our Privacy Notice and the Conditions of Use will change also. We may e-mail periodic reminders of our notices and conditions, but you should check our Web site frequently to see recent changes. Unless stated otherwise, our current Privacy Notice applies to all information that we have about you and your account. We stand behind the promises we make, however, and will never materially change our policies and practices to make them less pro-

pective of customer information collected in the past without the consent of affected customers.

Related Practices and Information

Conditions of Use

Discussion Boards

Community Rules

Help department

Most Recent Purchases

Your Profile and Community Guidelines

EXAMPLES OF INFORMATION COLLECTED

INFORMATION YOU GIVE US

You provide most such information when you search, buy, post, participate in a contest or questionnaire, or communicate with customer service. For example, you provide information when you search for a product; place an order through Amazon.com or one of our third-party sellers; provide information in Your Account (and you might have more than one if you have used more than one e-mail address when shopping with us) or Your Profile ; communicate with us by phone, e-mail, or otherwise; complete a questionnaire or a contest entry form; use our services such as Amazon Instant Video; compile Wish Lists or other gift registries; participate in Discussion Boards or other community features; provide and rate Reviews; and employ Product Availability Alerts, such as Available to Order Notifications. As a result of those actions, you might supply us with such information as your name, address, and phone numbers; credit card information; people to whom purchases have been shipped, including addresses and phone number; people (with addresses and phone numbers) listed in 1-Click settings; e-mail addresses of your friends and other people; content of reviews and e-mails to us; personal description and photograph in Your Profile ; and financial information, including Social Security and driver's license numbers.

AUTOMATIC INFORMATION

Examples of the information we collect and analyze include the Internet protocol (IP) address used to connect your com-

puter to the Internet; login; e-mail address; password; computer and connection information such as browser type, version, and time zone setting, browser plug-in types and versions, operating system, and platform; purchase history, which we sometimes aggregate with similar information from other customers to create features like Top Sellers ; the full Uniform Resource Locator (URL) clickstream to, through, and from our Web site, including date and time; cookie number; products you viewed or searched for; and the phone number you used to call our 800 number. We may also use browser data such as cookies, Flash cookies (also known as Flash Local Shared Objects), or similar data on certain parts of our Web site for fraud prevention and other purposes. During some visits we may use software tools such as JavaScript to measure and collect session information, including page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page. We may also collect technical information to help us identify your device for fraud prevention and diagnostic purposes.

MOBILE

Most mobile devices provide users with the ability to disable location services. Most likely, these controls are located in the device's settings menu. For information about specific devices, click here . If you have questions about how to disable your device's location services, we recommend you contact your mobile service carrier or your device manufacturer.

INFORMATION FROM OTHER SOURCES

Examples of information we receive from other sources include updated delivery and address information from our carriers or other third parties, which we use to correct our records and deliver your next purchase or communication more easily; account information, purchase or redemption information, and page-view information from some merchants with which we operate co-branded businesses or for which we provide technical, fulfillment, advertising, or other services; search term and search result information from some searches conducted through the Web search features offered by our subsidiary, Alexa Internet; search results and links, including paid listings (such as Sponsored Links); and credit history information from credit bureaus, which we use to help prevent and detect fraud and to offer certain credit or financial services to some customers.

CO-BRANDED AND JOINT OFFERINGS

Examples of businesses with which we offer joint or co-branded products and other offerings include Starbucks, OfficeMax, Verizon Wireless, Sprint, T-Mobile, AT&T, J&R Electronics, Eddie Bauer and Northern Tool + Equipment.

INFORMATION YOU CAN ACCESS

Examples of information you can access easily at Amazon.com include up-to-date information regarding recent orders; personally identifiable information (including name, e-mail, password, communications and personalized advertising preferences, address book, and 1-Click settings); payment settings (including credit card information and promotional certificate and gift card balances); e-mail notification settings (including Product Availability Alerts, Delivers, and newsletters); Recommendations (including Recommended for You and Improve Your Recommendations); shopping lists and gift registries (including Wish Lists and Baby and Wedding Registries); Seller accounts; and Your Profile (including your product Reviews, Recommendations, Listmania lists, Reminders, personal profile, and Wish List).

ANEXO VIII. TERMOS E CONDIÇÕES DE USO - ESPECÍFICO PARA ASSINATURA DO PRIME VIDEO PELAS CLIENTES VIVO

Estes Termos e Condições de Uso são aplicáveis aos Clientes Vivo que contrataram o serviço de vídeo da Amazon Prime Video (o "Serviço") por meio da TELEFONICA DATA S/A., empresa devidamente inscrita no CNPJ/MF sob o nº 04.027.547/0036-61, com sede na Av. Tamboré, nº 341, parte, Alphaville, Barueri-SP, denominada simplesmente "VIVO" ("Termos de Uso para Clientes VIVO") e são separadas e distintas do AMAZON PRIME VIDEO – TERMOS DE USO, denominado como "Termos de Uso do Prime Video" e localizado em <https://www.primevideo.com/region/na/help?nodeId=202095490> ou em outro local que a Amazon irá disponibilizar. Você precisa aceitar ambos os termos e condições do serviço para acessar e começar a utilização do serviço, sendo que, no que for conflitante, as disposições contidas neste Termo de Uso prevalecerão sobre as previstas no Termos de Uso do Prime Video.

I – Descrição do Serviço O Serviço permite acesso a filmes e séries para assistir quando e onde quiser! Conteúdos Prime Originals, filmes que são sucessos de bilheteria e séries exclusivas. Ao contratar o Serviço, serão aplicáveis os preços e condições estabelecidas nestes Termos de Uso para Clientes VIVO. A sua assinatura será renovada automaticamente mensalmente. II - Valor do Serviço: Ao contratar o Serviço, a cobrança da sua assinatura será automática e realizada: (a) em sua conta de VIVO, quando você tiver uma conta de celular pós-pago ou controle, banda larga, TV ou linha fixa, ou (b) mediante desconto de seus créditos, quando você tiver uma conta de celular pré-pago. Nome da Oferta Preço (R\$) Frequência Período degustação Amazon Prime Video 7,90 nos primeiros 6 meses, após 6 meses 14,90 Mensal 90 dias, uma única vez por Cliente III - Contratação e cancelamento: 1. Para Cliente com celular VIVO: você deve enviar uma mensagem SMS com a palavra AMAZON para o número 1060. Em seguida você receberá uma mensagem para confirmar a assinatura e você deverá responder à mensagem com a palavra SIM. Para Clientes de linha fixa, banda larga e/ou TV: você deve acessar a página da web <http://vivo.com.br/primevideo> ou ligar na central de atendimento VIVO 103 15. Pessoas com necessidades especiais de fala ou audição, podem ligar no número 142.2. O Cliente não deve possuir débito (valor vencido e não pago) junto a VIVO no momento da contratação do Serviço. 3. A contratação do Serviço somente poderá ser realizada pelo titular da fatura da linha fixa, TV, banda larga da VIVO ou seu representante devidamente autorizado. No caso de Clientes com plano (Móvel) a contratação será realizada por meio do dispositivo móvel que tenha conexão com a VIVO. Assim, a VIVO não se responsabiliza e/ou realiza qualquer confirmação da identidade daquele que está em posse do dispositivo móvel da VIVO e realiza a solicitação da assinatura do Serviço. No caso dos planos de linha fixa, TV e/ou banda larga o Cliente precisa entrar em contato com a central de atendimento VIVO e todos os dados do Cliente são validados pelo atendente.

4. Para cancelar a assinatura do Serviço no caso de Clientes com celular VIVO, o mesmo deverá enviar uma mensagem SMS com a palavra SAIR para o número 1060 ou entrar em contato com a VIVO por telefone no número *8486 ou 142 para pessoas com necessidades especiais de fala/audição, o serviço será interrompido na data do encerramento do período pago pelo Cliente, sem a opção de pró-rata. Para Clientes de linha fixa, TV e/ou banda larga o cancelamento do Serviço pode ser realizado através da central de atendimento VIVO através do número 103 15 ou 142 para pessoas com necessidades especiais de fala/audição, o serviço será interrompido na data da solicitação de cancelamento e o valor da mensalidade do serviço será apresentado em fatura proporcional aos dias de vigência da assinatura no modelo pró-rata. Não há fidelidade na contratação deste Serviço. 5. No caso de cancelamento pelo Cliente de seu celular, linha fixa, TV e/ou banda larga contratados junto à VIVO, a assinatura do Serviço será automática e imediatamente cancelada, não tendo o Cliente direito à devolução e/ou restituição dos valores já pagos pelo Serviço. 6. O período promocional para degustação é de 90 dias, e será disponibilizado uma única vez por Cliente, iniciando-se automaticamente a partir do primeiro dia da sua primeira assinatura.

ANEXO IX. TERMO DE TRATAMENTO DE DADOS PESSOAIS DA TELEFÔNICA

Versão 01 -01/07/2019

OBJETIVO

Este Termo de Tratamento de Dados Pessoais (“Termo”) se aplica aos tratamentos de dados pessoais realizado sem razão de Contrato de Prestação de Serviços e/ou Fornecimento(“Contrato”), celebrado por e entre CONTRATANTE e CONTRATADA, ambas definidas no Contrato,e o integra para todos os fins de direito.

2.DEFINIÇÕES

A CONTRATANTE e a CONTRATADA são doravante designadas, em conjunto, “Partes” e, individualmente, “Parte”. Não obstante qualquer disposição em contrário no Contrato, no caso de qualquer ambiguidade ou conflito entre os demais documentos integrantes do Contrato e deste Termo, os termos e condições deste Termo prevalecerão. Quaisquer termos iniciados em letras maiúsculas e não definidos de outra forma neste Termo terão o significado atribuído a eles no Contrato. Exceto conforme modificado abaixo, os termos do Contrato permanecerão em pleno vigor e efeito. “Anonimização”: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. “Controlador”: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, aqui representado pela CONTRATANTE. “Dado Pessoal”: dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa, bem como nome, prenome, estado civil, filiação e endereço, e-mail, telefone. “Dado Pessoal Sensível”: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. “Encarregado”: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados. “Incidente de Segurança”: o estabelecido na Cláusula 3.3.1. “Leis Aplicáveis”: toda a legislação brasileira, incluindo leis, regulamentos, regras, ordens, decretos ou outras diretrizes com força de lei, relacionadas à proteção de dados e que sejam aplicáveis às Partes. “Operador”: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, aqui representado pela CONTRATADA. Versão 01

-01/07/2019“Requisitos de Segurança”: requisitos mínimos de segurança da informação estabelecidos pela CONTRATANTE para Tratamento seguro dos Dados Pessoais. Estarão consolidados em documento anexo ao Contrato, caso a CONTRATANTE julgue aplicável.“Serviços”: os serviços e/ou fornecimentos, bem como outras atividades a serem executadas pela CONTRATADA à CONTRATANTE,ou em seu nome,nos termos do Contrato.“Subcontratado”: os subcontratados, representantes e outros prestadores de serviços terceirizados, pessoa natural ou jurídica, contratados pelo Operador, que tenham acesso a Dados Pessoais relacionados à execução do Contrato.“Titular”:pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.“Tratamento”:toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

3. OBRIGAÇÕES SOBRE A PROTEÇÃO DE DADOS

3.1.CONTROLADORA E OPERADORA

3.1.1.As Partes reconhecem que no âmbito da prestação dos Serviços a CONTRATANTE atuará na qualidade de Controladora, somente, e a CONTRATADA, conforme definido no preâmbulo, na qualidade de Operadora, conforme as obrigações e responsabilidades estabelecidas a cada uma delas, nos termos das Leis Aplicáveis.

3.2.TRATAMENTO DOS DADOS PESSOAIS

3.2.1.São obrigações da CONTRATADA no âmbito deste Termo:

3.2.1.1.Tratar os Dados Pessoais, conforme as instruções e diretrizes da CONTRATANTE, na medida do necessário para a prestação do Serviço. É vedado o Tratamento adicional de qualquer Dado Pessoal ao qual a CONTRATADA, por ventura, tenha acesso em razão do Contrato para outras finalidades, salvo se expressamente autorizado pela CONTRATANTE.

3.2.1.2.Manter e disponibilizar, quando solicitado pela CONTRATANTE, registro de todas as categorias de atividades de Tratamento realizadas em decorrência do Contrato, de acordo com as Leis Aplicáveis. Este registro deverá incluir, ao menos:a) A descrição dos processos de Tratamento de Dados Pessoais realizados.Versão 01 -01/07/2019 b)A relação de transferências de Dados Pessoais para fora do Brasil,quando expressamente autorizado pela CONTRATANTE,incluindo a identifi-

cação (i) dos países destino e (ii) do mecanismo de transferência utilizado para realização da transferência internacional.c) Descrição geral das medidas técnicas e organizacionais utilizadas pela CONTRATADA, conforme descrito nos Requisitos de Segurança, caso aplicável. d) Nome e dados de contato do Subcontratado, caso aplicável, assim como seus representantes ou Encarregado.

3.2.1.3.Auxiliar a CONTRATANTE a cumprir as obrigações estabelecidas nas Leis Aplicáveis, principalmente aquelas relacionadas aos direitos dos Titulares.

3.2.1.4.Comunicar imediatamente a CONTRATANTE caso os Titulares exerçam seus direitos perante a CONTRATADA, sendo vedada qualquer providência para atendimento de demanda de Titulares por parte da CONTRATADA sem autorização prévia e expressa da CONTRATANTE.

3.2.1.5. Fornecer à CONTRATANTE as informações necessárias para elaboração de documentos exigidos pelas Leis Aplicáveis em decorrência de Tratamentos de Dados Pessoais, especialmente o relatório de impacto à proteção de Dados Pessoais.

3.2.1.6.Permitir que a CONTRATANTE realize auditorias ou inspeções, por si ou por terceiros, a qualquer tempo, mediante comunicação prévia,a fim de verificar o cumprimento das obrigações dispostas neste Termo.

3.2.1.7.Excluir ou devolver à CONTRATANTE a critério da CONTRATANTE, todos os Dados Pessoais ao término do Contrato.

3.2.1.8.Designar um Encarregado da proteção de Dados e informar os seus contatos à CONTRATANTE, se exigível pelas Leis Aplicáveis.

3.3.INCIDENTE DE SEGURANÇA

3.3.1.A CONTRATADA deverá imediatamente notificar a CONTRATANTE: (i) se tiver conhecimento ou suspeitar de qualquer comprometimento, divulgação a pessoas não autorizadas ou uso de Dados Pessoais de maneira não autorizada; (ii) se tiverem sido apresentadas quaisquer reclamações sobre as práticas de tratamento pela CONTRATADA; ou (iii) se tiver ocorrido qualquer descumprimento significativo ou substancial deste Termo (cada um denominado individualmente "Incidente de Segurança").

3.3.2.A CONTRATADA deverá: (i) cooperar integralmente com a Versão 01 -01/07/2019 CONTRATANTE para a investigação do Incidente de Segurança incluindo, sem limitação, a disponibilização de servidores à CONTRATANTE ou ao representante por ela designado, para investigação forense com o intuito de determinar o escopo de qualquer Incidente de Segurança; e

(ii) preservar todas as informações e evidências relacionadas ao Incidente de Segurança incluindo, entre outros, a suspensão de limpeza (overwriting) ou exclusão rotineiras de dados ou arquivos de log.

3.3.3.A CONTRATADA deverá imediatamente reembolsar à CONTRATANTE todos os custos razoáveis incorridos pela CONTRATANTE para a resposta e/ou minimização do Incidente de Segurança decorrentes de, ou relacionados à, violação pela CONTRATADA de suas obrigações decorrentes do Contrato ou destes Termos

3.3.4.Salvo se exigido pelas Leis Aplicáveis ou compelida por uma intimação, ordem judicial ou outro documento legal similar emitido judicialmente ou pela Autoridade Nacional de Proteção de Dados, a CONTRATADA concorda em não divulgar o Incidente de Segurança a qualquer terceiro sem primeiramente obter o consentimento prévio e por escrito da CONTRATANTE.

3.3.5.A critério exclusivo da CONTRATANTE, na hipótese de um Incidente de Segurança decorrente de uma violação do Contrato, ou deste Termo, pela CONTRATADA, acarretar em necessidade: (i) de envio de uma notificação a autoridades públicas ou indivíduos; ou (ii) da adoção de outras medidas corretivas, se solicitado pela CONTRATANTE, a CONTRATADA deverá adotá-las às suas custas. O momento, conteúdo e maneira de realização de quaisquer notificações ou medidas corretivas serão determinados pela CONTRATANTE.

4. SUBCONTRATAÇÃO

4.1.É vedado à CONTRATADA compartilhar com, ou permitir o Tratamento por, terceiros de Dados Pessoais a que tiver acesso, em decorrência do Contrato, salvo se prévia, expressa e formalmente autorizado pela CONTRATANTE.

4.2.Caso haja subcontratação autorizada pela CONTRATANTE, a CONTRATADA permanecerá responsável por todas as obrigações contidas neste Termo, incluindo:

4.2.1.Informar à CONTRATANTE a identidade e localização do Subcontratado, bem como a descrição do Tratamento pretendido.

4.2.2.Tomar as medidas cabíveis para garantir o cumprimento deste Termo pelo Subcontratado, aplicando a ele as mesmas obrigações e responsabilidades aqui dispostas.

4.3.A CONTRATADA é solidariamente responsável pelo Tratamento de Dados Pessoais realizados pelo Subcontratado, respondendo por eventuais danos causados por este.

Aplicação da Lei de Proteção de Dados Pessoais: um estudo de caso de apps de empresas com modelo de negócio baseado em dados

Tradução da pesquisa “Aplicación de la Ley de Protección de Datos Personales en Brasil: estudio de caso de algunas empresas con modelo de negocio basado em datos” escrita por Kimberly Anastácio, Bruna Santos e Joana Varon, realizada pela Coding Rights como parte da publicação “Festín de Datos: Empresas y datos personales en América Latina”, por Vivian Newman Pont, Daniel Ospina-Celis e Juan Carlos Upegui.

Autoras Kimberly Anastácio, Bruna Santos e Joana Varon

Coordenadora do Projeto - Coding Rights Joana Varon

Coordenador do Projeto - DeJusticia Daniel Ospina

Design Clarote

Data da Publicação Rio de Janeiro, Junho 2020.

Publicação Coding Rights | contato@codingrights.org



Esse texto está disponível para download em www.codingrights.org