



MARCELLO WILKER DOS SANTOS MOTA

**A INVISIBILIDADE DOS DATA BROKERS À LUZ DO REGULAMENTO
GERAL DE PROTEÇÃO DE PROTEÇÃO DE DADOS:
INCOMPATIBILIDADE OU INEFICÁCIA DA LEGISLAÇÃO?**

Tese com vista à obtenção do grau de
Mestre em Direito na especialidade
Direito Social e da Inovação

Orientador:

Doutor Fabrizio Esposito, Professor da Faculdade de Direito da
Universidade Nova de Lisboa

Setembro de 2023



NOVA SCHOOL OF LAW

**A INVISIBILIDADE DOS DATA BROKERS À LUZ
DO REGULAMENTO GERAL DE PROTEÇÃO DE
PROTEÇÃO DE DADOS: INCOMPATIBILIDADE
OU INEFICÁCIA DA LEGISLAÇÃO?**

Setembro
2023

DECLARAÇÃO ANTIPLÁGIO

Declaro por minha honra que o trabalho que apresento é original e que todas as minhas citações estão corretamente identificadas. Tenho consciência de que a utilização de elementos alheios não identificados constitui uma grave falta ética e disciplinar.

AGRADECIMENTOS

Aos meus familiares que sempre estiveram comigo nesta jornada, em especial, à minha tia Val Santos sem a qual nada disto seria possível, obrigado por acreditar em mim e por sempre me motivar.

Ao meu orientador com o qual tive o prazer de receber instruções e que não mediu esforços para que este trabalho pudesse ser concluído.

Aos meus colegas e amigos de Mestrado Gabriel Oliveira, Isabella Neves, Ítala Luz, João Teixeira e Júlia Felipe por terem tornado esta jornada mais leve e divertida.

Um agradecimento especial à Tiago Salgado que me acompanhou na construção deste trabalho e que foi de enorme contributo para a sua bibliografia, sempre com um bom café ao lado e com palavras de motivação.

RESUMO

Com o advento da internet, indivíduos estão mais conectados e a sociedade está cada vez mais imersa em uma economia baseada em dados. Com acesso a serviços, principalmente online, uma enorme quantidade de dados é gerada, o que tem atraído o interesse de empresas como os data brokers. Estas empresas coletam informações pessoais sobre indivíduos, as processa e os classifica de acordo com diversos parâmetros como, por exemplo, comportamentais, econômicos etc. Após enriquecer os dados ou classificar os indivíduos, brokers vendem as informações para diversos setores econômicos com as mais distintas finalidades. Com o objetivo de garantir maior proteção aos indivíduos, o Regulamento Geral de Proteção de Dados estabelece uma série de critérios e princípios a serem obedecidos no tratamento de dados pessoais. Naturalmente, esta normativa impacta diretamente a atividade dos data brokers que têm como característica a falta de transparência e, em muitos casos, o tratamento ilícito de dados pessoais. Há um certo interesse por parte das autoridades controladoras em regular esta atividade em razão dos riscos que expõem os titulares. O Regulamento e demais legislações complementares podem ser ferramentas importantes para salvaguardar os direitos dos titulares, todavia, podem não ser suficientemente eficazes para regular a atividade dos data brokers.

Palavras-chaves: Dados pessoais - Titulares - Regulamento Geral de Proteção de Dados.

ABSTRACT

With the internet, individuals are more connected and society is increasingly immersed in a data-driven economy. With access to services, especially online, a huge amount of data is generated, which has attracted the interest of companies such as data brokers. These companies collect personal information about individuals, process it and classify it according to various parameters, such as behavioral, economic, etc. After enriching the data or classifying individuals, brokers sell the information to different economic sectors for different purposes. In order to ensure greater protection for individuals, the General Data Protection Regulation establishes a series of criteria and principles to be obeyed in the processing of personal data. Naturally, this regulation directly impacts the activity of data brokers, which are characterized by a lack of transparency and, in many cases, the illicit processing of personal data. There is some interest on the part of controlling authorities in regulating this activity due to the risks to which data subjects are exposed. The Regulation and other complementary legislation can be important tools to safeguard the rights of holders, however, they may not be effective enough to regulate the activity of data intermediaries.

Key words: Personal data - Data subjects - General Data Protection Regulation.

SUMÁRIO

INTRODUÇÃO	7
1. CONTEXTUALIZAÇÃO	8
1.1. O que são Data Brokers.....	8
1.2. Data Brokers e o Regulamento Geral de Proteção de Dados	10
1.3. Fontes de Dados.....	13
1.4. Data Brokers e o Tratamento de Dados Pessoais para Fins de Marketing Direto.....	16
1.5. Modelo de Negócio	20
1.5.1. Vigilância.....	21
1.5.2. Pesquisa	25
1.5.3. Coleta.....	29
1.5.4. Análise	31
1.5.5. Sintetização e apresentação da informação.....	33
2. DATA BROKERS SOB ANÁLISE.....	34
2.1. Efeitos colaterais inerentes à sua atividade	34
2.1.1. Rastreamento excessivo	34
2.1.2. Falta de transparência	36
2.1.3. Discriminação.....	38
2.1.4. Exposição de dados.....	39
2.1.5. Manipulação.....	40
2.1.6. Processamento invisível	41
2.1.7. Desvio de finalidade.....	43
2.1.8. Uso malicioso de dados pessoais.....	45
2.1.9. Supressão da liberdade de expressão e acesso à informação	47
2.1.10. Acusações injustas e opressão por autoridades legais	48
2.2. Estudo de caso: avaliação de políticas de privacidade.....	49
2.2.1. Equifax	50
2.2.2. Oracle.....	53
2.2.3. Experian	55

2.2.4. Conclusão	57
3. FRAMEWORK LEGAL: LEGISLAÇÃO E DAS DECISÕES DAS AUTORIDADES DE CONTROLE. ANÁLISE JURÍDICA DA ATIVIDADE DOS DATA BROKERS	58
3.1. REGULAMENTO DE GOVERNAÇÃO DE DADOS	58
3.2. DIRETRIZES 05/2020 RELATIVAS AO CONSENTIMENTO NA ACEÇÃO DO REGULAMENTO 2016/679	62
3.3. PROPOSTA DE REGULAMENTO RELATIVO À PRIVACIDADE E ÀS COMUNICAÇÕES ELETRÔNICAS (DOCUMENTO 52017PC0010)	66
3.4. DIRETIVA 93/13 RELATIVA ÀS CLÁUSULAS ABUSIVAS NOS CONTRATOS CELEBRADOS COM OS CONSUMIDORES	69
3.4. ENTENDIMENTO DAS AUTORIDADES DE CONTROLE	72
CONCLUSÃO	76
REFERÊNCIAS BIBLIOGRÁFICAS	77

INTRODUÇÃO

Em uma sociedade cada vez mais digital, milhões de dados pessoais são gerados a todo o momento por indivíduos ao acessar serviços. Há o estabelecimento de uma relação comercial entre acesso à domínios online ou serviços em troca da recolha de dados, todavia, esta relação nem sempre se dá de forma transparente. A economia está se moldando e se tornando cada vez mais digital, onde dados pessoais são uma commodity de grande valor uma vez processados e enriquecidos.

A comercialização de dados pessoais está no cerne da atividade dos data brokers que exploram este lucrativo mercado. O seu modelo de negócio é estruturado para uma coleta massiva de dados pessoais oriundos de diversas fontes, públicas ou privadas, onde nem sempre há uma relação direta com os seus titulares/consumidores.

Como forma de garantir a proteção aos indivíduos, o Regulamento Geral de Proteção de Dados (RGPD) é uma peça fundamental na economia baseada em dados ao estabelecer que o processamento de dados pessoais seja feito de forma transparente, lícita e segura. Todavia, mesmo com o advento do RGPD, data brokers ainda são capazes de atuar sem enfrentar muitas barreiras, mesmo com o um modelo de negócio que aparenta ir na contramão da legislação.

Em que pese a enorme quantidade de dados processados bem como os riscos inerentes a natureza da atividade dos data brokers, atualmente, estas empresas têm passado despercebidas aos olhos do legislador, mesmo impactando a vida de milhões ao redor do globo e, em especial, na União Europeia enfoque deste trabalho.

O presente estudo tem como enfoque a relação da atividade dos data brokers com o RGPD e qual o papel deste instrumento, juntamente com as demais

normas que formam o atual framework jurídico principalmente em torno da base legal do consentimento para o processamento de dados dos titulares/consumidores, para a regulação das atividades daquelas empresas.

1. CONTEXTUALIZAÇÃO

1.1. O que são Data Brokers

Data brokers ou informational brokers são empresas ou pessoas físicas que coletam, vendem ou licitam dados pessoais¹ (RODRIGUES, 2020). Estes dados são coletados de fontes públicas ou, comprados de outras empresas. A origem destas empresas vem de antes da era da internet com a introdução do sistema de credit scores para determinar a credibilidade de pessoas privadas (CORESIGNAL, 2022). Nos anos 80 empresas começaram a aprender mais a respeito de seus consumidores ao coletar informações detalhadas e criar uma base de dados (CHRISTIL e SPIEKERMANN, 2016). Os dados pessoais processados eram e ainda são, em muitos casos, obtidos de outras fontes que não sejam os seus titulares e sim através de outras empresas ou domínios públicos para que sejam futuramente vendidos (FORBRUKERRADET, 2020).

Com o advento da internet que acelerou a globalização, houve um expressivo aumento na quantidade de dados gerados pelos usuários, aumento este que desde então se mantém acelerado. As pessoas estão constantemente

¹ Artigo 4º, n.1, Regulamento Geral de Proteção de Dados (RGPD) "«Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular". (Disponível em <<https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>>. Acessado em 12.09.2022).

gerando centenas de milhares de dados que são dispersos na internet. Tais dados contêm informações valiosas a respeito de seus donos, e é de interesse das empresas ter acesso a elas.

Dados pessoais se tornaram uma commodity de enorme valor agregado (BIRCKAN; DUTRA; MACÊDO; VIEIRA, 2020) que despertaram grande interesse comercial para a sua obtenção. Para Jammet (2014), quanto mais dados pessoais são adquiridos por uma empresa, maior será a sua receita. Entretanto, na sociedade globalizada em que vivemos e no modelo econômico vigente, não há mais tempo para uma empresa coletar e processar os dados que considera relevante para o seu modelo de negócio e ainda garantir sua competitividade no mercado (CHRISTOZOV e TOLETA-STOIMENOVA, 2014). Em muitos casos, ao desempenhar esta atividade por si própria resulta em uma expressiva quantidade de tempo, dinheiro e risco de terem aqueles dados obsoletos antes da conclusão do trabalho de coleta e processamento, pois na era da internet, a informação está sempre em movimento e tendências a mudarem constantemente.

Em virtude de muitos dos dados pessoais estarem publicamente disponíveis o seu processamento se revela um desafio, soma-se a isto o fato de haver dados que precisam ser comprados de fontes privadas. Para suprir a falta de tempo, data brokers têm uma grande relevância no sistema econômico, pois, ao usarem de seu conhecimento especializado são capazes de fornecer os dados pessoais relevantes para propósitos específicos. Estas empresas podem se especializar em um mercado específico tais como marketing, mitigação de riscos, financeiro, etc.

Através do uso de data mining, dados crus são transformados em informações que podem ser utilizadas de forma estratégica para atender os objetivos de uma empresa (FIA, 2021). Data brokers analisam dados com a finalidade de identificar potenciais consumidores, projeções e mitigar riscos ao descobrir padrões em uma grande quantidade de dados com o uso de

metodologias oriundas da estatística, e reconhecimento de padrões (CHRISTIL e SPIEKERMANN, 2016).

1.2. Data Brokers e o Regulamento Geral de Proteção de Dados

A coleta de dados pessoais não pode se dar de forma indiscriminada. Por conterem informações que podem ainda ser sensíveis², data brokers têm de lidar com elas de forma responsável e respeitar o direito de privacidade de seus donos (CORESIGNAL, 2022). Devido a natureza da atividade dessas empresas, é natural que aumente o interesse na sua regulamentação pelos Estados.

É esperado que por se tratar de processamento de dados pessoais, esta atividade tenha que obedecer a certos instrumentos jurídicos. O RGPD é atualmente, o principal ordenamento jurídico a impor regras que devem ser observadas por todos os agentes que lidam com dados pessoais dos residentes na União Europeia.

Tal Regulamento traz em seu artigo 5º os princípios relativos ao processamento de dados pessoais³:

- a) Licitude, lealdade e transparência: os titulares dos dados pessoais devem ser informados a respeito do seu tratamento, a razão da sua

² De acordo com o IMY., dados sensíveis são aqueles que "(...) reveals a person's race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and personal data concerning a person's health and sex life. Data concerning health may for example comprise sick leave, pregnancy and doctor's visits. Handling such data is normally prohibited but there are exceptions. Sensitive personal data must also be protected more than other data." (Disponível <<https://www.imy.se/en/individuals/data-protection/introduktion-till-gdpr/what-is-actually-meant-by-personal-data/what-is-meant-by-sensitive-personal-data/>>. Acessado em 12.09.2022).

³ Disponível em <<https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>> Acessado em 12.09.2022.

recolha bem como, as empresas devem ser leais ao fim informado aos titulares para o seu uso e observar a sua adequação legal⁴;

- b) Limitação das finalidades: a recolha dos dados pessoais deve ter finalidades determinadas, explícitas e legítimas a serem seguidas durante todo o seu processamento;
- c) Minimização dos dados: o tratamento será limitado aos dados estritamente necessários às finalidades estabelecidas;
- d) Exatidão: os dados devem ser exatos e atualizados sempre que necessário, as empresas devem zelar pela sua atualização;
- e) Limitação da conservação: devem ser conservados por um período que seja estritamente necessário para o cumprimento das finalidades estabelecidas, podem ainda ser conservados por um período maior em alguns casos como, por exemplo, para fins de interesse público;
- f) Integridade e confidencialidade: deve ser assegurada a segurança no tratamento de dados pessoais, os protegendo contra o tratamento não autorizados ou ilícitos; devem ser adotadas medidas técnicas e organizacionais adequadas;
- g) Responsabilidade: quem tratar dados pessoais é responsável pelo cumprimento dos demais princípios e deve comprová-lo.

Data brokers devem ter não somente os princípios em mente quando do tratamento de dados pessoais⁵, mas sua atividade deve ainda se encaixar em uma das justificativas legais para o processamento.

⁴ As empresas devem observar a adequação legal do tratamento. (Disponível <https://www.sgs.pt/pt-pt/news/2021/11/rgpd-7-principios-fundamentais>. Acessado em 13.09.2022).

⁵ Artigo 4º, n.2, RGPD “«Tratamento», uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição”. (Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Acessado em 12.09.2022).

O artigo 6º do RGPD determina quando o tratamento de dados pessoais é legal. Entre as justificativas estão o consentimento; a necessidade para execução de um contrato ou uma obrigação jurídica; necessário ao exercício de funções públicas, etc.

O consentimento dado pelos titulares pode caracterizar a principal justificativa para o tratamento de dados pessoais pelos data brokers. Todavia, este consentimento por si só pode não ser o suficiente para a coleta e processamento, pois deve estar alinhado com os princípios que norteiam o tratamento de dados pessoais.

Se, mesmo após a obtenção do consentimento não for possível implementar as medidas técnicas e organizacionais necessárias para garantir, por exemplo, proteção contra acessos ou transferências não autorizados, o tratamento não observará o que determina o RGPD.

Importante também salientar que, quando do pedido de consentimento, este deve se dar de maneira clara que permita ao titular identificar a finalidade do tratamento e quem está fazendo-o, devendo ainda ser assegurado o direito de retirada do consentimento (artigo 7º, RGPD). Na mesma esteira está a extensão do consentimento. A partir do fato de que, à primeira vista, o titular apenas conhece e dá o seu consentimento para a empresa/domínio com a qual está interagindo diretamente, quando esta transfere os dados pessoais para um data broker no qual o titular desconhece, as condições originais do consentimento ficam abaladas o que pode em tese, prejudicar o direito do titular de retirar o seu consentimento. Esta impossibilidade se encontra ainda relacionada com outra questão, a de que uma vez dado, o titular dos dados não tem uma forma simples de rastrear para quem deu consentimento e/ou quem está a tratá-los, limitando assim o direito de acesso previsto no artigo 15º do RGPD.

1.3. Fontes de Dados

O tratamento de dados pessoais se dá em diferentes categorias e tem diferentes propósitos. Como mencionado, dados pessoais podem ser destinados para setores como o de marketing, financeiro, saúde, ciência, etc. Para cada setor haverá data brokers especializados para prover os dados que são relevantes para o fim pretendido.

Como há diferentes categorias de dados e, portanto, diferentes tipos de data brokers, é comum que haja o comércio de dados pessoais entre data brokers para obter informações mais corretas e precisas ao combinar os dados obtidos de diferentes fontes (BERGMANIS-KORATS; TWETMAN, 2021).

De acordo com o relatório elaborado pelo Concelho do Consumidor Norueguês (FORBRUKERRADET, 2020), data brokers processam dados de fontes online e offline para criar perfis que revelam informações detalhadas a respeito dos consumidores e criam uma versão gêmea digital deste indivíduo que poderá ser vendida ou licenciada para outras empresas.

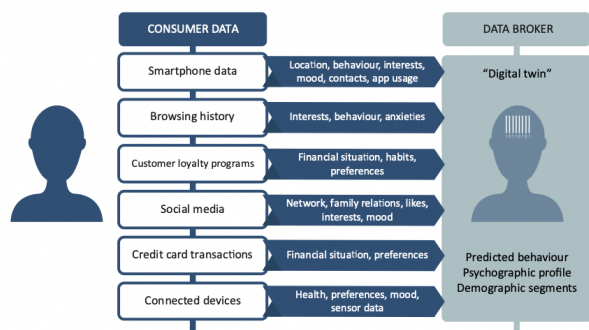


Figura 1: “Digital twin”⁶

⁶ Disponível em <<https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf>>, p. 21. Acessado em 12.09.2022.

O relatório elaborado por BERGMANIS-KORATS e TWETMAN (2021) para a NATO intitulado “Data brokers and security. Risks and vulnerabilities related to commercially available data”, aponta ainda para uma subdivisão das fontes de dados que podem ser:

a) Públicas

Composta por informações demográficas, certidões de nascimento, casamento, listas telefônicas, licenças profissionais, registros criminais, lista de insolventes, dados de censos, etc.

Fontes públicas são exemplos de dados que podem ser tratados de forma offline. Tais registros geralmente têm como controllers entidades públicas como notários, hospitais e tribunais de justiça que podem ser consultados de forma gratuita⁷. O uso de fontes públicas é comum entre data brokers em razão da quantidade significativa de dados que esta fonte obtém e da sua relevância para o mercado.

b) Fontes comerciais: histórico de compras, informações de crédito, informações de cartões fidelidade, etc.;

c) Rastreamento online: perfis em redes sociais, aplicativos de smartphones, websites, cookies, plugs, etc.

Com a internet, dados oriundos de fontes online se tornaram mais comuns e volumosos. Uma das fontes mais utilizadas são os smartphones, principalmente em razão dos aplicativos que podem ser neles instalados pelos seus usuários. De acordo com o relatório elaborado por CHRISTL e SPIERMANN (2016) intitulado Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy, smartphones usam

⁷ “The data controller determines the purposes for which and the means by which personal data is processed”. (Disponível em <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en>. Acessado em 25.09.2022).

diversos tipos de conexões para transferência de dados, tais como WLAN, GSM, 4G, Bluetooth, etc., e são equipados com uma gama de sensores que permitem a geração de dados.

Estes aparelhos possuem em seu sistema operacional aplicações básicas que permitem a realização de ligações, criação de agenda telefônica, acesso à câmera fotográfica, etc., também é possível a instalação de aplicativos disponíveis nas lojas oficiais de acordo com o software do dispositivo (Android ou IOS). Estes aplicativos, por sua vez, requerem permissão para acessar diferentes sensores presentes nos smartphones que podem ser desde acesso a agenda telefônica ou localização de GPS onde dependendo do tipo de aplicação, estas permissões são indispensáveis para o seu funcionamento. Um aplicativo de navegação como Waze, precisa ter acesso a localização GPS para que forneça a melhor rota para o destino pretendido pelo usuário. O mesmo se aplica ao Instagram quando o usuário fornece sua localização para fazer check-in em determinado lugar, ou permite o acesso à câmera e/ou galeria de fotos.

Tal permissão não se limita apenas ao uso de aplicativos, uma vez que há domínios online que requerem permissão para o armazenamento de informações sobre o usuário. Em certos casos, é possível o titular dos dados fazer a escolha de suas preferências com relação ao que pode ou não ser analisado, entretanto, ainda há permissões que não podem ser negadas. A negativa por parte do consumidor com relação ao tratamento de seus dados pessoais pode ter como consequência o não acesso ao domínio ou que sua experiência no mesmo seja prejudicada.

O rastreamento online tem como grande contributo a informação gerada e cedida pelos próprios titulares em uma espécie de escambo digital, ao molde do que acontecia no período colonial, por exemplo, entre Brasil e Portugal, onde havia a troca de produtos entre portugueses e os indígenas. Nos tempos

atuais, isto se dá na forma de permissão/consentimento para o tratamento de dados pessoais em troca de acesso a plataformas digitais ou à informação.

1.4. Data Brokers e o Tratamento de Dados Pessoais para Fins de Marketing Direto

Como anteriormente mencionado, o uso de data brokers ou a prática do data broking para marketing direto se traduz na coleta de em diferentes fontes de dados sobre consumidores e combinar as informações obtidas. De acordo com a Information Commissioner's Office (ICO.,2018), os serviços para propósito de marketing direto podem incluir:

- a) Venda de lista de contatos telefônicos;
- b) Venda de cópias de registros eleitorais;
- c) Enriquecimento de dados (adicionar informações a perfis já existente em bancos de dados de empresas);
- d) Combinação de dados (por exemplo, providenciar números telefônicos de pessoas das quais uma empresa apenas tem parte da informação, podendo ser endereço eletrônico);
- e) Limpeza de dados e rastreamento (apagar dados obsoletos dos registros para possibilitar o rastreo de novos).

A construção do banco de dados para marketing teve como grande aliado para sua implementação o programa de fidelidade implementado pela American Airlines em 1981 (CHRISTL; SSPIEKERMANN, 2016). Estes programas ainda contribuem para a base de dados, todavia, a internet transformou a forma como dados pessoais são coletados para identificar potenciais consumidores. Meta Platforms Inc., é atualmente uma das empresas que mais lucram com propagandas direcionadas com base em dados pessoais (CALIF, 2022). Um estudo realizado por DEIGHTON e

JOHNSON (2013) aponta que o data-driven marketing baseado em dados de consumidores a nível individual, teve um lucro de pelos menos \$156 bilhões de dólares somente nos Estados Unidos.

O relatório Networks Of Control aponta o fato de que data brokers não levam em conta os riscos que a exposição e compartilhamento de dados pessoais podem representar aos seus titulares, e chama este fenômeno de “Customer’s Lifetime Risk”⁸. Tais fenômeno compila e categoriza potenciais riscos que os titulares/consumidores podem enfrentar durante e depois do processo de tratamento de seus dados pessoais.

Há fatores apontados no mencionado relatório que podem contribuir com os riscos nos quais os titulares são expostos, tais como:

- a) Duração da transferência de dados;
- b) Número de empresas com as quais os dados são compartilhados;
- c) Medidas de segurança adotadas pelo titular;
- d) Direitos de privacidade e regulação seguidos pelo coletor dos dados.

Entre os riscos nos quais os titulares estão sujeitos devido ao compartilhamento de seus dados pessoais, baseado no fenômeno do “Customer’s Lifetime Risks” e, em observação ao estudo elaborado por Daniel J. SOLOVE (2006, p. 81) intitulado “A Taxonomy of Privacy” Cit., por CHRISTL e SPIEKERMANN (2016) ⁹, foi criada a seguinte tabela não exaustiva:

⁸ De acordo com este fenômeno “risco podem ser baseados na licitude ou ilicitude do uso de dados do consumidor; riscos podem resultar do próprio consumidor ou da empresa que está lidando com dados pessoais e; riscos podem se relacionar com várias dimensões de consequências negativas”. (Disponível em <https://crackedlabs.org/dl/Christl_Spiekermann_Networks_Of_Control.pdf, pg. 80. Acessado em 12.09.2022).

⁹ Disponível em <https://crackedlabs.org/dl/Christl_Spiekermann_Networks_Of_Control.pdf>, p. 81. Acessado em 12.09.2022).

Discriminação	☐ Discriminação de preços ☐ Discriminação de oferta ☐ Acesso limitado a garantia ☐ Acesso limitado a crédito ☐ Dados sem contexto que podem levar a: ○ Deturpações e falsas conclusões ○ Julgamentos injustos baseados em dados falsos ou ultrapassados
Manipulação	☐ Ser visado quando vulnerável ☐ Controle de comportamento (com recompensas/punições) ☐ Informação de campanhas personalizadas com interesses políticos ou comerciais
Ameaças de Segurança	☐ Roubo de identidade ☐ Uso ilícito de dados pessoais ☐ Ataques cibernéticos ☐ Perda e vazamento de informações ☐ Quebras de confidencialidade
Mudanças Sociais	☐ Alterações de comportamento ○ Autocensura ○ Inibição ☐ Conformismo ☐ Inibição de impactos em ○ Criatividade ○ Liberdade de expressão

	○ Autonomia individual – autodesenvolvimento e autodeterminação □ Digital wildfires (propagação de conteúdo danoso em mídias sociais) □ Auto valoração ou de outros baseada em dados □ Habilidade de falar e de agir anonimamente é exibida por métodos □ “Problemas arquitetônicos” – danos sistemáticos e estruturais, causando o aprimoramento de riscos ou uma mudança no equilíbrio do poder social ou institucional
Privacidade Individual	□ Divulgação pública de fatos privados e secretos □ Revelação de informação além da expectativa do usuário □ Uso indevido e disseminação de dados sem o consentimento (informado) do usuário □ Perseguição, constrangimento, monitoramento cibernético □ Propagação de informações falsas ou enganosas e rumores □ Exposição, condenação □ Danos de reputação □ Chantagens □ Propagandas invasivas (spam, pop ups ou telemarketing)

Desequilíbrios de Marketing	❑ Espionagem industrial ❑ Criação de monopólios ❑ Menos diversidade de mercado ❑ Falta de transparência ❑ Vantagens para economias nacionais onde servidores são abrigados ❑ Injusta prática de informação por consumidores ○ Conhecimento limitado sobre a existência de bancos de dados ○ Habilidade limitada de revelar qual informação é registrada e como é usada ○ Habilidade limitada de corrigir ou emendar o registro de informação identificável
---	--

1.5. Modelo de Negócio

De acordo com CHRISTOZOV e TOLEVA-STOIMENONA (2014), o modelo de trabalho de um data broker consiste nas seguintes etapas:

1.5.1. Vigilância

Informação é gerada pelos mais diversos meios de interação como compras online, redes sociais, utilização de aplicativos, etc.¹⁰. Por meio da informação disponível, data brokers podem rastrear o comportamento e preferências dos indivíduos como, por exemplo, preferências religiosas, políticas ou estilo de vida.

Como salienta SAMPAIO (2017), a sociedade vive uma “hipervigilância digital” dos dados postos à disposição (online ou offline) através de dispositivos ou histórico de navegação. Para DIJCK (2014), este fenômeno se dá por meio de “dataveillance”¹¹ que, ao contrário da vigilância que monitora dados para um propósito específico, faz um rastreo muito mais abrangente e agressivo.

É notório que a vigilância vai de encontro com certos princípios do RGPD como, por exemplo, a licitude, lealdade e transparência, a limitação das finalidades e a minimização dos dados. O princípio da licitude (artigo 5º, 1, a, do RGPD) prega que para o tratamento de dados pessoais é preciso uma razão justificável e legítima e só vai ser lícito quando se verifique ao menos uma das seguintes situações constantes no artigo 6º do RGPD:

- a) Consentimento;

¹⁰ Toda a informação gerada, quer online ou offline, é observada através do uso de algoritmos e convertida em códigos que irão alimentar o banco de dados para marketing.

¹¹ DIJCK conceitua dataveillance como “the monitoring of citizens on the basis of their online data—differs from surveillance on at least one important account: whereas surveillance presumes monitoring for specific purposes, dataveillance entails the continuous tracking of (meta)data for unstated present purposes (...). Dataveillance is thus a far-reaching proposition with profound consequences for the social contract between corporate platforms and government agencies on the one hand citizens-consumers on the other (...)”. p. 9. (Disponível em <<https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/datafication/datafic>>. Acessado em 17.09.2022).

- b) Execução de um contrato;
- c) Cumprimento de uma obrigação jurídica;
- d) Defesa dos interesses vitais do titular dos dados ou de outra pessoa singular;
- e) Exercício de funções de interesse público ou exercício da autoridade pública;

Na etapa da vigilância os dados pessoais são tratados de forma indiscriminada, sem finalidade determinada e na contramão do que determina o princípio da licitude, lealdade e transparência uma vez que, nesta fase, há um tratamento de uma massiva quantidade de dados oriundos de fontes online e offline, não há a garantia do consentimento dado pelos seus titulares que, por sua vez, podem nem estarem cientes de que estão sendo vigiados. O mesmo pode se aplicar quanto a existência de um contrato em razão da falta de conhecimento do tratamento se traduzir na inexistência de um contrato celebrado diretamente com data brokers.

É notório que a atividade exercida pelos data brokers se mostra à margem da legislação já em sua fase inicial. Não é possível observar nenhuma das bases legais descrita no artigo 6º do RGPD.

O Regulamento determina ainda que o tratamento de dados pessoais deve ter finalidades determinadas, explícitas e legítimas a serem seguidas durante todo o tratamento e que não podem ser tratados posteriormente de forma incompatível com os parâmetros já definidos conforme prega do artigo 5º, 1, b do RGPD. Para além da finalidade explícita, o tratamento deve se ater ao princípio da minimização dos dados pelo qual serão tratados apenas aqueles dados pessoais estritamente necessários à finalidade ou finalidades estabelecidas. A definição da finalidade é essencial para estabelecer os limites do tratamento bem como quais serão as medidas mais apropriadas para garantir a segurança dos dados. Este é um procedimento que deve ser

adotado antes que o tratamento seja iniciado, conforme determina o artigo 25º, 1, do RGPD:

Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados.

Não há qualquer discriminação na primeira etapa do modelo de funcionamento dos data brokers, não importa qual método utilizado, haverá sempre o tratamento de mais dados do que seria necessário (FRAZÃO, 2019). Pode-se afirmar que “necessidade” não se aplica à esta etapa, pois para saber qual a necessidade para o tratamento de dados é imperioso o estabelecimento de um propósito específico com o fim de terminar as regras para a sua realização, o que não existe na vigilância.

A falta de transparência no tratamento de dados por data brokers é alvo de grande preocupação conforme apontou a Federal Trade Commission (FTC) norte-americana no relatório intitulado “Data Brokers: A Call for Transparency and Accountability” (BRILL; MCSWEENEY; OHLHAUSEN; RAMIREZ e

WRIGHT, 2014), uma vez que o tratamento pode envolver dados sensíveis como raça, opiniões políticas, crenças religiosas ou filosóficas, associações etc.

A transparência no tratamento de dados está no cerne do RGPD dada a categoria de direito na qual a proteção destes dados se enquadra. O Considerando 1 do Regulamento o classifica como um direito fundamental que está presente no artigo 8º,1, da Carta dos Direitos Fundamentais da União Europeia¹². Nesta esfera, MENEZES (2021) Apud SUSSEKIND (2001) aponta cinco direitos fundamentais do indivíduo provenientes da informática:

- a) Direito à intimidade: limitação no tratamento dos dados para fins específicos;
- b) Direito à confidencialidade: coibir o acesso às informações por aqueles que não tiverem legitimidade;
- c) Direito de acesso às informações coletadas sobre si: para observação da extensão e exatidão dos dados;
- d) Direito de correção e exclusão de informação inexata;
- e) Direito à prescrição de informações que possam ser danosas.

Ressalta-se ainda que o direito à intimidade se encontra resguardado no artigo 12 da Declaração Universal dos Direitos Humanos que defende “Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem ataque à sua honra e reputação etc.”¹³. A vigilância constitui também uma violação ao direito à intimidade dos consumidores uma vez que informação gerada por smartphones, por

¹² “Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito”. (Disponível em <<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR>>. Acessado em 12.09.2022)

¹³ Disponível em <<https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>>. (Acessado em 13.09.2022).

exemplo, é alvo de tratamento. Essa violação, traduz-se na limitação dos direitos apontados por MENEZES (2021) e previstos no artigo 5º do RGPD. Nesta etapa, o exercício do direito ao apagamento ou retificação de dados inexatos pode ser prejudicado quando não há conhecimento a respeito de seu tratamento. Surge então uma contradição: o avanço tecnológico tem permitido acesso quase instantâneo à informação, de forma prática através de dispositivos como smartphones, e possibilita que os usuários da grande rede tenham mais consciência do que está acontecendo ao seu redor (quer a nível local ou global) ao mesmo passo que, veem se tornando cada vez menos cientes que a informação por eles gerada, está sendo tratada para fins e por uma duração que desconhecem.

1.5.2. Pesquisa

Enquanto na etapa da vigilância há o tratamento indiferenciado dos dados gerados, sem um propósito específico, aplicando-se a máxima do Big Data¹⁴ onde a intenção é tratar a maior quantidade de dados possível, na etapa da pesquisa é aplicado um filtro ao tratamento.

A pesquisa nas fontes de dados se dá a partir do ponto de vista da relevância e acessibilidade dos dados (CHRISTOZOV e TOLEVA-STOIMENOVA, 2014). Como data brokers vendem dados pessoais para clientes de setores como, por exemplo, marketing ou financeiro, nesta etapa será levado em consideração os dados que melhor atendem aos interesses do cliente. Se o data broker é especializado no tratamento de dados voltados para o setor

¹⁴ De acordo com a Rocketcontent, big data “é o conjunto de informações presentes nos bancos de dados de servidores e empresas, que pode ser acessado e possui interligações entre si.” (Disponível em <<https://rockcontent.com/br/blog/big-data>>. Acessado em 03.10.2022).

financeiro, os dados pessoais relevantes a serem pesquisados serão aqueles que revelem o status do seu titular e determinem o risco financeiro de lhe oferecer crédito (PYLES, 2020).

Parte dos dados financeiros estão disponíveis em domínios públicos, por exemplo, em Portugal é possível ter acesso a lista de pessoas e empresas que se encontram em processo de execução através do portal Citius, para isso, bastam informações simples como o nome do titular, informação esta que pode ser obtida através da etapa de vigilância.

Na pesquisa, o preço para o acesso aos dados também é relevante, logo, não é de causar espanto que o tratamento de dados provenientes de fontes públicas e gratuitas podem ser de grande relevância aos data brokers, uma vez que poderão a partir deles, obterem lucro sem precisar pagar pela informação. De acordo com o BERGANIS-KROATS e TWETMAN (2021), o processo de compra de acesso vai depender do tipo de informação que está sendo pesquisada, quanto mais detalhada a informação, maior poderá ser o seu valor.

Muitos data brokers atuam dentro da legalidade no tratamento de dados pessoais ao usar informações públicas e ao comprar o acesso a fontes privadas, mas que ainda sim possuem legitimidade para armazenar tais dados. Todavia, também há o mercado negro de dados pessoais. Este mercado possui data brokers especializados no tratamento deste tipo de informação de forma ilegal, mas que podem ser os mesmos que atuam legalmente no processamento de dados pessoais.

Dados pessoais comercializados no mercado negro possuem grande relevância aos data brokers e podem ser desde detalhes de log-in, informações de cartão de crédito a dados sensíveis como registros médicos. O mercado negro de dados é alimentado, mas não exclusivamente, por hackers e criminosos cibernéticos (BERGANIS-KROATS e TWETMAN,2021).

Ressalta-se que o RGPD dedica especial atendimento no que se refere a dados sensíveis no artigo 9º como, por exemplo, a previsão do consentimento dado pelo titular dos dados ser explícito.

Como demonstrado, um dos grandes problemas na atuação dos data brokers é a falta de transparência na sua atuação, o titular dos dados pessoais na maioria das vezes não está ciente de que seus dados estão a ser tratados, por isso, não dá o seu consentimento informado para tal.

O Considerando 39 do Regulamento diz que¹⁵:

O tratamento de dados pessoais deverá ser efetuado de forma lícita e equitativa. Deverá ser transparente para as pessoas singulares que os dados pessoais que lhes dizem respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados. O princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples.

Se não há conhecimento sobre o tratamento, não há como garantir o acesso aos dados pelos titulares, o que constitui uma violação ao Regulamento. Na mesma esfera, quando é pedido o consentimento, este deve seguir algumas regras, como ser apresentado de forma clara e concisa utilizando linguagem de fácil compreensão, bem como especificar como os dados serão utilizados etc. No que tange ao acesso à informação, de acordo com o artigo 13º, 1, do

¹⁵ Diposníel em <<https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1559280280904&uri=CELEX:32016R0679#d1e1690-1-1>>. Acessado em 03.10.2022).

RGPD o responsável pelo recolhimento tem a faculdade de informar ao titular dos dados:

- a) A identidade da organização a efetuar o tratamento dos dados;
- b) A finalidade do tratamento;
- c) O tipo de dados que serão tratados;
- d) A possibilidade de desistir do consentimento dado;
- e) Se aplicável, o fato de os dados irem ser utilizados para decisões exclusivamente automatizadas, incluindo definições de perfis;
- f) Eventual transferência internacional dos dados e os possíveis riscos relacionados à transferência para fora da União Europeia.

Quanto ao consentimento explícito, a Guidelines 05/2020 on Consent under Regulation 2016/679 do European Data Protection Board¹⁶, diz que:

The term explicit refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent. An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement. Where appropriate, the controller could make sure the written statement is signed by the data subject, in order to remove all possible doubt and potential lack of evidence in the future.

¹⁶ Disponível em
<https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf>, p. 20. Acessado em 03.10.2022).

Em que pese o Regulamento não clarificar o momento em que o consentimento deve ser dado, a regra geral é que isto deve acontecer antes do tratamento a exemplo do que ocorre com a especificação do propósito para o tratamento¹⁷. Como acontece na etapa da vigilância, na pesquisa pelos dados relevantes, data brokers comumente atuam sem o consentimento informado ou explícito por parte dos consumidores que não têm a mínima informação sobre o tratamento e, portanto, não podem exercer os seus direitos que deveriam ser garantidos pelo Regulamento. Percebe-se que a incompatibilidade entre o RGPD e a atividade exercida por data brokers também é evidente na segunda etapa do seu modelo de atuação. A falta de transparência tolhe os titulares dos dados pessoais de exercer seus direitos fundamentais.

1.5.3. Coleta

Superada a fases de tratamento de dados, inicia-se a coleta da informação relevante. Como mencionado, data brokers procuram por dados pessoais em fontes públicas e privadas. A coleta pode ser feita através de distribuição de materiais gratuitos que os titulares dos dados pessoais concordam em receber como, por exemplo, e-books (MACEDO, 2022) ou ao concordarem em receber ofertas de emprego entre outros tipos de materiais que podem ser recebidos via e-mail ou postal.

A internet torna a coleta de dados online muito mais constante e dinâmica. Os dados gerados através de e-mails, redes sociais, dispositivos eletrônicos

¹⁷ De acordo com a Opinion 15/2021 on the definition of consent “Although the timing for seeking consent is not spelt out in the Directive, it is clearly implied from the language of the various provisions which indicate that, as a general rule, consent has to be given before the processing starts (...). (Disponível em <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf>, p. 9. Acessado em 03.10.2022).

que já haviam sido vigiados e pesquisados agora estão prontos para serem coletados. Para além da coleta por meio da distribuição de materiais, há a que também é feita com a utilização de cookies utilizados por domínios online para o armazenamento de informações sobre os usuários¹⁸. Neste meio de coleta, o titular dos dados pessoais dá o seu consentimento para o tratamento. Somente aqui é possível observar um certo alinhamento entre a atividade dos data brokers e o RGPD no que tange a licitude do tratamento com base no consentimento (artigo 6º, 1, a) e por consequência, ao princípio da transparência (artigo 5º, 1, a) uma vez que o titular dos dados é informado sobre o seu processamento.

Importante pontuar também o fato de ainda que a coleta por meio de cookies se dá com o consentimento, este nem sempre é necessário. Há casos de cookies que não exigem o consentimento dado pelo titular dos dados como, por exemplo, os utilizados para proceder à transmissão de uma comunicação ou que sejam estritamente necessários para fornecer um serviço ou ainda, cookies de autenticação. É de se esperar ainda que, mesmo sem a necessidade do consentimento, outros princípios presentes no artigo 5º do Regulamento sejam observados pelos data brokers. O consentimento deve ser dado por meio de um pedido apresentado em uma linguagem simples e clara que permita ao titular perceber, por exemplo, a finalidade do tratamento, quem irá realizá-lo, por quanto tempo os dados serão tratados, etc.

Outra forma de coleta se dá por meio de jogos online. Há uma vasta gama de jogos oferecidos de forma gratuita facilmente acessados pelos consumidores através de websites ou em lojas oficiais presentes em smartphones como,

¹⁸ Etiquetas de software que são armazenadas nos dispositivos através do navegador (browser), retendo informações relacionadas as preferências/permissões do usuário. (Disponível em < <https://www.techtudo.com.br/noticias/2018/10/o-que-sao-cookies-entenda-os-dados-que-os-sites-guardam-sobre-voce.ghtml>>. Acessado em 22.11.2022).

por exemplo, Apple Store. Esta facilidade de acesso aos jogos faz com que dados pessoais provenientes de crianças sejam processados por data brokers.

Há regras específicas para a coleta de dados de crianças. O Considerando 38 do RGPD diz que crianças podem estar menos cientes dos riscos, consequências e garantias com relação aos seus direitos em detrimento do tratamento dos seus dados pessoais. Em complemento, o Considerando 58 afirma que a comunicação de tratamento entregue às crianças deve ser redigida uma linguagem clara e simples que seja facilmente compreendida. Tais Considerandos são complementados pelo artigo 8º do RGPD que trata especificamente do consentimento obtido de crianças. Nestes casos, o consentimento do progenitor ou tutor vem antes do consentimento da criança (Regulamento (UE) 2016/679) e, a depender do país, a idade em que o titular dos dados é considerado como criança pode variar entre os 13 e os 16 anos¹⁹.

1.5.4. Análise

A habilidade de identificar a melhor ideia para solucionar a problemática analisada e apresentá-la ao mercado requer um conhecimento e metodologia especializados. É por esta razão que data brokers têm desenvolvido um papel de relevância econômica a suportar a dinâmica do mercado. Toda a

¹⁹ De acordo com a Comissão Europeia “As empresas têm de realizar esforços razoáveis, tendo em conta a tecnologia disponível, para verificar se o consentimento dado está efetivamente em conformidade com a lei. Tal pode envolver a aplicação de medidas de verificação da idade como por exemplo, fazer uma pergunta que a maioria das crianças não seja capaz de responder ou exigir que o menor forneça o endereço de correio eletrónico do progenitor para a obtenção do consentimento por escrito”. (Disponível em <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-personal-data-about-children-be-collected_pt>). Acessado em 05.10.2022).

informação tratada e coletada precisa ser analisada do ponto de vista da relevância, confiança, consistência etc. (CHRISTOZOV e TOLEVA-STOIMENOVA, 2014).

Ao fazer o processamento dos dados pessoais, indivíduos têm seus hábitos/tendências mapeados com o uso de algoritmos (BRICKAN; DUTRA; MACEDO e VIREIRA, 2020) que permitem a criação de um perfil para cada usuário. É esta informação final que é vendida ao mercado. É como se esta commodity fosse um diamante bruto que é lapidado pelos data brokers e vendidos a quem estiver neles interessado.

Uma informação tem mais valor de mercado quando ela é exata no sentido de traçar um perfil sobre o seu titular. Se termos em consideração data brokers especializados no setor de marketing, por exemplo, os dados analisados sobre os seus titulares serão aqueles capazes de revelar seus comportamentos enquanto potenciais consumidores que irão receber propagandas especializadas e direcionadas aos seus gostos revelados a partir do seu histórico de navegação ou “likes” em redes sociais.

Tendo como exemplo uma empresa que queira lançar determinado produto, é importante que tenha o conhecimento a cerca do comportamento e intenções do mercado, saiba a quem poderá direcionar propagandas e para isto é necessária uma análise especializada de uma enorme quantidade de dados. Data brokers irão fazer a análise dos dados relevantes que foram coletados para, por exemplo, categorizar os titulares de dados pessoais que poderão ser potenciais consumidores do produto.

Nesta etapa, o princípio da exatidão dos dados utilizados do RGPD se faz presente. Como visto, tal princípio prega que os dados pessoais devem ser exatos e atualizados bem como sejam adotadas medidas adequadas a garantir que dados inexatos sejam retificados ou apagados sem demora (artigo 5º, 1, d). Novamente a atividade dos data brokers se mostra potencialmente violadora.

Tendo em vista a falta de transparência no tratamento de dados pessoais sem o consentimento de seus titulares, estes eventualmente não poderiam exercer o direito de retificação de dados inexatos ou mesmo que eles fossem apagados. Um data broker pode montar um perfil sobre determinado consumidor com base em dados inexatos e vende-lo a uma empresa que o enxerga como um potencial cliente e irá lhe enviar programada através, por exemplo, de e-mail. Por sua vez, o titular que agora foi classificado como eventual consumidor irá se deparar com uma empresa desconhecida lhe enviando propaganda sobre um produto no qual não tem interesse em decorrência da inexatidão dos dados utilizados para traçar o seu perfil. Exigir a correção da inexatidão ou, que os seus dados sejam apagados pode ter como barreira a eventual impossibilidade de saber onde aquela empresa conseguiu os dados (data broker) e, ter como consequência a incapacidade de exercer o seu direito, o que implica em uma direta violação ao princípio da exatidão.

1.5.5. Sintetização e apresentação da informação

Nesta última etapa, toda a massiva quantidade de dados vigiados indiscriminadamente na etapa inicial, já passou por várias fases de refinamento e não se encontra mais no seu estado bruto, pois já foram traçados os parâmetros relevantes para o seu tratamento. Pela sintetização, a informação será resumida para servir os interesses do cliente para quem será apresentada, ou seja, ensinada (CHRISTOZOV e TOLEVA-STOIMENOVA, 2014). Tendo como exemplo a empresa que deseja lançar um produto, ao final desta etapa poderá vir a ter acesso a informações referentes ao potencial público consumidor tais como endereço de e-mail, estilo de vida e capacidade econômica.

2. DATA BROKERS SOB ANÁLISE

2.1. Efeitos colaterais inerentes à sua atividade

Dada a natureza de sua atividade e modelo de negócio, há potenciais riscos nos quais titulares de dados pessoais estão sujeitos. Por esta razão, há um grande interesse dos Estados em regular esta atividade. Algumas agências que visam a proteção dos dados pessoais de seus residentes como, por exemplo, o Conselho do Consumidor Norueguês, a FTC nos Estados Unidos, bem como a ICO, têm emitido relatórios nos quais se dedicam a uma análise profunda deste mercado e apontam danos oriundos do processamento de dados pessoais. Nas próximas sessões, serão apontados alguns destes estudos quais corroboram com a linha de pesquisa do presente estudo.

Commented [A1]: Referencia.

Regla: em casos como isso, cita fontes

Commented [MM2R1]: Done

2.1.1. Rastreio excessivo

De acordo com o relatório da FORBRUKERRADET (2020), muitos consumidores não se sentem confortáveis com o rastreio online de seus dados e de serem categorizados. Estudos têm mostrado que consumidores têm se revelado insatisfeitos com a quantidade de propaganda recebida.

O relatório cita que muitos titulares acham que o rastreio de dados pessoais não é ético e que apenas um pequeno número concorda em ser rastreado em ordem de receberem melhores produtos e serviços (FORBRUKERRADET, 2020). De acordo com os estudos, há um maior desejo por parte dos titulares de exercer mais poder sobre os seus dados pessoais e restringir o seu processamento para finalidades outras que não sejam as originalmente informadas e consentidas.

Esta excessividade também leva à violação de privacidade com data brokers tendo o acesso a muitos dados sensíveis o que aumenta o risco de exposição dos seus titulares (BERGMANIS-KORATS; TWETMAN, 2021) que podem sofrer constrangimentos em algum momento de suas vidas por conta da informação processada por data brokers.

O rastreo excessivo de dados pessoais reflete na perda de poder de decisão de seus usuários. Isto se revela em muitos casos desde a sua coleta sem o conhecimento do titular, o que pode resultar em propagandas direcionadas indesejadas, no desvio de finalidade do processamento dos dados pessoais, etc. Outra consequência pode ser o sentimento de insegurança, já que há estudos que revelam que consumidores estão cada vez mais preocupados com o fato de terem sua localização rastreada (FORBRUKERRADET, 2020). Outra consequência do rastreo excessivo pode ser a diminuição da concorrência no mercado de dados, onde empresas que tenham uma política de privacidade mais alinhada com o RGPD e, portanto, respeitem os direitos dos titulares, podem estar em desvantagem com relação as que têm como objetivo a maximização dos lucros com a recolha agressiva de dados pessoais, tornando difícil a entrada no mercado por data brokers que tentem limitar o processamento alinhado com os princípios do Regulamento (BEUC, 2019). Como já mencionado, dados pessoais possuem grande valor agregado uma vez categorizados e, quanto maior a quantidade de dados processados por data brokers mais dominante será a sua posição no mercado o que põe em desvantagem aqueles que tenham o intento de seguirem um modelo de negócio “privacy-friendly” (FORBRUKERRADET, 2020).

2.1.2. Falta de transparência

Transparência no processamento de dados pessoais é um dos princípios do RGPD sendo assim, um direito dos titulares que se aplica “independentemente se o dado pessoal é obtido diretamente do indivíduo ou de outras fontes” (ICO, 2020)²⁰.

Em uma investigação realizada pela ICO. em 2020 que findou no relatório intitulado “Investigation into data protection compliance in the direct marketing data broking sector”, identificou sérias falhas na proteção de dados pessoais no banco de dados das maiores agências de referência de crédito do Reino Unido (Experian, Equifax e TransUnion).

De acordo com ICO., as agências de referência providenciavam algumas informações sobre como realizavam o processamento e suas fontes de dados, todavia, de forma vaga que não permitia a compreensão clara de como a atividade era realizada.

A falta de transparência pode acarretar em um grande desequilíbrio de poder entre indivíduos e empresas, uma vez que elas podem deter uma quantia significativa de dados pessoais que seus titulares nem sequer estão cientes (FORBRUKERRADET, 2020). Tal fato se mostra visível nos casos em que os dados são compartilhados com terceiros, quando os titulares em muitos casos não entendem a natureza e profundidade do seu consentimento para usar certo domínio (BERGMANIS-KORATS; TWETMAN, 2021).

Outro ponto que contribui com a falta de transparência é que grande parte dos dados obtidos por data brokers têm como origem outros data brokers (BRILL; MCSWEENEY; OHLHAUSEN; RAMIREZ e WRIGHT, 2014). Tal

²⁰ Disponível em <<https://ico.org.uk/media/action-weve-taken/2618470/investigation-into-data-protection-compliance-in-the-direct-marketing-data-broking-sector.pdf>>. Acessado em 22.02.2023

prática resulta em um ciclo vicioso de que uma vez coletado, dados pessoais passam de data brokers à data brokers que os passam a empresas (o que é permitido pelo RGPD se observados os princípios da transparência, licitude do tratamento etc.) e que podem ser novamente coletados por data brokers ou compartilhados com outras empresas e assim por diante, formando uma rede complexa de tráfego que torna quase impossível ao titular saber quem processou ou quem está processando seus dados pessoais. Isto pode se dar em virtude do fato de não haver uma previsão no RGPD sobre a extensão do consentimento (quando a coleta original se deu por meio de tal), no sentido de quando o titular dos dados consente que eles sejam tratados por um broker ou empresa ou, consentir com o compartilhamento entre terceiros, não há um limite sobre até onde o consentimento dado para a coleta/compartilhamento original pode se estender, o que acaba por abrir uma brecha para este ciclo de coleta e compartilhamento desenfreado. Cria-se assim, uma certa contradição na legislação, pois ao mesmo tempo em que o RGPD prega a transparência e a minimização no tratamento dos dados, não se aprofunda de forma eficaz sobre quais seriam as limitações para o tratamento.

A consequência do desequilíbrio de poder entre data brokers e indivíduos é a própria incapacidade dos titulares se protegerem de não terem seus dados processados e serem categorizados ou, de exercer o seu direito a correção de dados imprecisos e/ou que os mesmos sejam apagados em sua totalidade, tal como ter a capacidade de realizar o rastreamento do compartilhamento de seus dados pessoais.

Commented [A3]: Is this legal, in your view? Why?

Commented [MM4R3]: Mentioned that the GDPR does allow this, if the principles of transparency, lawfulness etc. are met. This is further explored on chapter 3 dedicated to the legal analysis.

2.1.3. Discriminação

Em virtude de data brokers coletarem muito mais dados do que o necessário desde a primeira etapa do seu modelo de negócio, é inevitável e até mesmo intencionado que os mesmos processem dados sensíveis inclusos nas categorias especiais de dados mencionadas no artigo 9º do RGPD. O relatório da FTC chama atenção ao fato de que as análises de dados feitas por data brokers para fazer inferências sobre seus titulares. O uso de dados sensíveis acarreta na criação de categorias que têm como base informações relacionadas a orientação sexual, raça, escolaridade (BRILL; MCSWEENY; OHLHAUSEN; RAMIREZ e WRIGHT, 2014).

Titulares dos dados coletados por data brokers podem ter suas vidas afetadas em razão desta atividade sem nem ao menos estarem cientes disso. Com base na informação processada por estas empresas, consumidores que, após serem categorizados, podem ter seu pedido de financiamento recusado, ter que arcar com planos de saúde mais caro ou enfrentar dificuldades em ter acesso aos mesmos ou, em caso de exposição desses dados sofrerem discriminação se, por exemplo, forem portadores de alguma doença estigmatizada pela sociedade.

O relatório da FTC traz à tona o testemunho feito por Pam Dixon, diretor executivo da World Privacy Forum no Congresso dos Estados Unidos onde relatou que data brokers oferecem listas de categorias com base em dados extremamente sensíveis tais como vítimas de estupro ou portadores de doenças genéticas (BRILL; MCSWEENY; OHLHAUSEN; RAMIREZ e WRIGHT, 2014). O uso de informações deste gênero para, por exemplo, marketing direto pode causar transtornos aos destinatários no que tange ao risco de reviver/relembrar uma experiência que lhes foi traumatizante ou que lhes causou dor como, por exemplo, o caso citado no relatório da NATO onde um consumidor recebeu uma carta promocional da empresa OfficeMax que

continha a sentença “filha morta em um acidente de carro”, fazendo com que o recipiente revivesse a dor da perda da filha um ano depois de sua morte. Mensurar a quantidade de dados processados por data brokers é quase impossível, até mesmo para os próprios já que um dos seus objetivos é coletar a maior quantidade de dados pessoais possível. Ao categorizar os titulares com base nos dados obtidos os coloca em uma posição de extrema desvantagem, pois, a depender de como foram classificados podem ter suas vidas diretamente afetadas de forma negativa por tais práticas como enfrentar barreiras de acesso à serviços de saúde, financiamento, reviver traumas etc., e isto ocorre em muitos casos sem nem ao menos saber como isto ocorre.

2.1.4. Exposição de dados

Devido ao fato de armazenarem uma imensa quantidade de dados pessoais, data brokers se tornam alvo cobiçado de hackers, uma vez que tais empresas possuem uma fraca política de cybersegurança (LEONG; YI-LING, 2020). A exposição de dados causados por uma quebra de segurança coloca os seus titulares em grande risco. Em 2017, umas das maiores agências de referência de crédito e data brokers Equifax, sofreu uma exposição de dados que afetou milhões de pessoas²¹. De acordo com o Identity Theft Resource Center (IRTC), em 2022 mais de 400 milhões de pessoas tiveram seus dados vazados, sendo mais da metade tiveram como origem o Twitter (GRIFFITH, 2023).

²¹ De acordo com o portal da Equifax “In September of 2017, Equifax announced it experienced a data breach, which impacted the personal information of approximately 147 million people. A federal court approved a class action Settlement that resolves lawsuits brought by consumers after the data breach. Equifax denied any wrongdoing and no judgment or finding of wrongdoing was made.” Disponível em WWW:<URL<https://www.equifaxbreachsettlement.com>>.

Os riscos relacionados a exposição de dados podem ter consequências severas, como o uso dos dados vazados para o cometimento de fraudes, roubo de identidade ou outros propósitos maliciosos. De acordo com a NATO, a falta de políticas de segurança põe em risco a privacidade e dados sensíveis de bilhões de pessoas em risco (BERGMANIS-KORATS; TWETMAN, 2021).

2.1.5. Manipulação

Data brokers podem manipular indivíduos ao usarem seus dados pessoais para influenciar seu comportamento ou decisões. Tal risco é oriundo da combinação entre Big data e psicologia comportamental (FORBRUKERRADET, 2020). Indivíduos podem ser alvo de marketing manipulativo para adquirirem produtos ou serviços e até mesmo serem alvo de manipulação política com base na informação que foi coletada sobre eles (BERGMANIS-KORATS; TWETMAN, 2021).

Data brokers podem vender dados políticos para empresas ou organizações que tenham interesse em propaganda direcionada²². Um estudo realizado pela Tactical Tech, baseado em estudo de casos ao redor do globo, descreve alguns dos métodos para manipulação política (TECH, 2019):

- a) Apps oficiais de campanhas solicitando permissão de acesso a câmera e microfone na Índia;
- b) Apps de porta-a-porta para prospecção identificando eleitores conservativos em mapas na França;

²² “(...) wider range of assertions that are made when interpreting the political relevance of data and the nature of consent – for example, how data point on the type of car you own or the fact that you have a low credit rating may be utilized to interpret and predict your political opinions.” Disponível em WWW:<URL <https://cdn.ttc.io/s/tacticaltech.org/Personal-Data-Political-Persuasion-How-it-works.pdf>>.

- c) Quebra de 55 milhões de dados sobre eleitores registrados nas Filipinas;
- d) Controle de impressões de eleitores a votarem pela primeira vez com ataques de propagandas e mecanismos de busca no Quênia;
- e) Uso de experimentação para selecionar slogans que desencadeassem respostas emocionais dos eleitores do Brexit.

Um dos casos mais famosos envolvendo manipulação é o escândalo da Cambridge Analytica onde, com base em dados obtidos através do Facebook identificava eleitores indecisos ou apoiadores de candidatos adversários considerados facilmente influenciados a ficarem em casa, e os alveja com mensagens os desencorajando de votar (BERGMANIS-KORATS; TWETMAN, 2021).

Está claro o grande poder que data brokers detêm e como podem impactar a vida dos indivíduos com o uso malicioso dos dados pessoais coletados e afetar diretamente direitos civis como liberdade de escolha ou direito ao voto, direitos inerentes a indivíduos que podem ser tolhidos com práticas escusas e por de trás dos bastidores.

2.1.6. Processamento invisível

O artigo 14 do RGPD prega²³:

3. O responsável pelo tratamento comunica as informações referidas nos nº 1 e 2:

²³ Disponível em [WWW:<URLhttps://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>](https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679)

- a) Num prazo razoável após a obtenção dos dados pessoais, mas o mais tardar no prazo de um mês, tendo em conta as circunstâncias específicas em que estes forem tratados;
- b) Se os dados pessoais se destinarem a ser utilizados para fins de comunicação com o titular dos dados, o mais tardar no momento da primeira comunicação ao titular dos dados; ou
- c) Se estiver prevista a divulgação dos dados pessoais a outro destinatário, o mais tardar aquando da primeira divulgação desses dados.

Se, após a coleta de dados por meio de terceiros o titular não for informado, ocorre o chamado “processamento invisível”, pois o titular não está ciente de que seus dados foram coletados e estão sendo usados por aquela empresa (ICO., 2020). De acordo com o relatório da ICO., as pessoas nem sempre têm uma relação direta com a data brokers, pois na grande maioria os dados coletados têm outras fontes (públicas ou privadas) que não sejam os próprios titulares dos dados pessoais, sendo identificado que data brokers não informam os titulares que seus dados foram indiretamente coletados e estão sendo usados para fins de marketing.

O relatório mencionado acima aponta ainda que as agências de referência de crédito justificam sua conduta com base na exceção prevista no artigo 14 (5) (a) que aluz o fato do titular já tenha conhecimento das informações, ou seja, da coleta de seus dados pessoais o que revela que as agências/data brokers baseiam-se na política de privacidade de terceiros que os fornecem dados. Tal fato se mostra problemático pois uma empresa geralmente não sabe as finalidades de tratamento de outra, ou seja, se o titular consente que seus dados sejam tratados para determinado fim, não terá como saber se esta

finalidade será respeitada por todas as empresas que vierem a processar seus dados pessoais.

O processamento invisível também é justificado por data brokers em razão do excessivo esforço que envolve informar cada indivíduo quando seus dados são processados por terceiros devido a grande quantidade de dados processados, o que cairia na exceção prevista no artigo 14 (5) (b) do RGPD (ICO, 2020). Tal prática se alinha com a falta de transparência já mencionada anteriormente e impacta diretamente os consumidores e seu poder de exercer os direitos previstos no Regulamento o que acentua ainda mais a incompatibilidade entre a atividade dos data brokers e o RGPD.

Commented [A5]: What is your legal analysis of these defenses?

Commented [MM6R5]: Explored on chapter 3

2.1.7. Desvio de finalidade

Com a investigação realizada pela ICO, pode-se perceber que a finalidade para tratamento pode mudar da inicialmente consentida pelo titular para outra diversa, e isto pode acontecer nos casos em que há interação direta entre o indivíduo e data broker ou quando esta interação é indireta por meio do compartilhamento de informações entre data brokers.

Na aludida investigação foi constatado que os data brokers processavam dados pessoais para uma finalidade diferente da inicialmente consentida. No caso em questão, data brokers que atuam no setor financeiro utilizavam dos dados pessoais processados para fins de marketing, enviando propaganda direcionada de acordo com o perfil financeiro do titular (ICO, 2020). Na mesma esteira, o Conselho do Consumidor Norueguês relata o mesmo fato, mas no sentido oposto, dados coletados para fins de marketing sendo utilizados para fins seguros ou crédito scoring (FORBRUKERRADET, 2020).

Essa mudança de finalidade não parece alinhar com o RGPD, uma vez que o Considerando 32^{aluz} que²⁴:

(...) O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins (...).

Tendo em vista que a complexidade que é a indústria de data broker (BRILL; MCSWEENEY; OHLHAUSEN; RAMIREZ e WRIGHT, 2014) se o titular tentar rastrear quem está processando seus dados e as finalidades do processamento poderá acabar em um labirinto e não ser hábil de achar tal informação pois, data brokers podem não informar que os dados coletados podem ser processados para finalidades diversas ou por não informar claramente com quem irá partilhar ou com quem partilhou os dados pessoais fornecendo um claro caminho para que o titular possa realizar o rastreio de suas informações (ICO., 2020). O que se pode inferir deste fato é que, como mencionado anteriormente, data brokers podem se basear nas exceções do artigo 14 do RGPD, principalmente na que refere ao esforço que envolve informar cada titular sobre como seus dados estão sendo processados e com qual finalidade, todavia, tendo em vista que o que está em causa é a transparência exigida para o processamento de dados pessoais, essa exceção não deveria ser facilmente garantida, caso contrário validaria todas as violações ao RGPD relacionadas com a atividade dos data brokers.

²⁴ Disponível em [WWW:<URLhttps://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>](https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679)

2.1.8. Uso malicioso de dados pessoais

Como apontado pela NATO, a atividade exercida por data brokers é preocupante por possuir problemas estruturais e não ser regulada (BERGMANIS-KORATS; TWETMAN, 2021), daí o interesse de governos em tentar regulá-la sendo o RGPD um grande avanço neste sentido, todavia, tem-se mostrado ineficiente.

A combinação entre a enorme quantidade de dados pessoais armazenados e uma fraca segurança põe data brokers em uma posição tentadora para cyber ataques (LEONG; YI-LING, 2020). Todos os anos há relatos de data breaches e, em que pese em 2022 ter havido menos casos que em 2021, a quantidade de dados pessoais expostos foi muito maior (GRIFFITH, 2023). O intuito primário de hackers que invadem bancos de dados de data brokers é de lucrar com eles como no caso do LimeLeads que, em 2019 foi alvo de hackers e 49 milhões de contatos empresariais foram postos à venda (CIMPANU, 2020).

Data brokers podem ainda serem utilizados por agentes com intenção de causar danos aos titulares dos dados pessoais, como fraude, roubo de identidade, ou para persegui-los em caso de Estados hostis (por exemplo, ser de interesse do Estado ter informações sobre críticos do governo ou rivais políticos) ou por grupos terroristas como apontado pela NATO (BERGMANIS-KORATS; TWETMAN, 2021).

Tal uso pode ter como origem acesso ilegal a bancos de dados através de hacking ou pelo acesso legal ao mesmo por meio de vazamento ocasionado por uma fraca segurança ou treinamento dos agentes que manipulam tais dados ou até mesmo por sua comercialização. Priorizar lucros e negligenciar medidas organizacionais que garantam proteção aos dados pessoais coletados, processados e armazenados põe seus titulares em uma posição

de grade risco, já que estão expostos a diversas ameaças e apenas realizam isto quando seus dados são expostos ou são vítimas de ações criminosas.

Poder ter a capacidade de entregar serviços mais adequados aos interesses das pessoas é uma das vantagens trazidas por data brokers, no entanto, o processamento de uma grande quantidade de dados que sobre indivíduos e o aumento no número de agentes que têm acesso aos mesmos, elevam os riscos dos titulares serem alvos de práticas maliciosas (FORBRUKERRADET, 2020). Com a exposição de dados armazenados pela Equifax, milhões de pessoas foram afetadas com a divulgação de informações como endereços, números telefônicos, informações sobre cartões de crédito, etc., entretanto, mesmo após tamanha exposição, os titulares não podem optar pela exclusão de seus dados (FTC, 2022). Em 2019 bilhões de dados pessoais foram expostos, ficando a disposição para quaisquer agentes e para as mais diversas finalidades, inclusive maliciosas. Um dos exemplos mencionados pela Comissão Norueguesa do Consumidor é o caso envolvendo o aplicativo de encontros Grindr destinado à comunidade LGBTQI+, onde os usuários foram localizados por Estados onde a homossexualidade é ilegal (FORBRUKERRADET, 2020).

Tal risco poderia ser diminuído se houvesse uma maior conscientização dos indivíduos sobre a importância dos seus dados combinado com a aplicação de medidas organizacionais mais eficientes para garantir a sua proteção. Todavia, se não há transparência sobre o tratamento, é mais difícil tornar os titulares cientes sobre a forma como fornecem dados e/ou sobre o que está sendo feito deles ou ter ciência de seus direitos.

2.1.9. Supressão da liberdade de expressão e acesso à informação

Ao passo que comumente indivíduos não estão cientes que seus dados estão sendo processados e utilizados para categorizá-los em diferentes perfis que serão vendidos para os mais diversos fins, quando há ciência ou desconfiância de qual fato ocorre, há uma moderação no seu comportamento referente a produção de dados pessoais (FORBRUKERRADET, 2020). Tal percepção pode ser desencadeada, por exemplo, quando um consumidor ao pesquisar por passagens aéreas na internet, começa a receber propagandas relacionada a hotéis, pacotes de viagem, etc.

O rastreo excessivo de dados pessoais pode fazer com as pessoas fiquem temerosas em usar a internet por receio de serem taxadas com base no seu histórico de navegação e serem alvo de práticas discriminativas. Tendo em vista o aspecto do consumidor, tal receio pode se transmitir na hesitação em comparar preços de determinados bens ou serviços pela crença de terem os preços ajustados de acordo com o fluxo da pesquisa (FORBRUKERRADET, 2020).

Na mesma esteira, tendo em base a ciência do rastreo pelo titular, o mesmo pode hesitar em emitir suas opiniões políticas ou religiosas por receio de repressão por parte de Estados mais opressores. Esta premissa também pode ser aplicada no que tange ao acesso à informação sobre sintomas ou tratamentos para determinada doença, se o titular acreditar que pode ter que enfrentar planos de saúde ou seguro de vida mais caros.

Estes receios podem prejudicar a confiança que as pessoas têm no mercado digital (FORBRUKERRADET, 2020), pois tendem a limitar seu acesso ao mundo digital o que pode ocasionar outra consequência, a exclusão. Em razão de vivermos em uma sociedade cada vez mais digitalizada, indivíduos que limitem interagir com este universo podem ser excluídos ou, como aponta a Comissão Norueguesa do Consumidor, se cada vez mais pessoas se

mostrarem descontentes com a forma em que seus dados pessoais são rastreados e processados e reduzirem sua interação com serviços digitais, haverá menos interesse em investir em inovações.

2.1.10. Acusações injustas e opressão por autoridades legais

Quando se pensa nos riscos envolvidos com a atividade exercida por data brokers é muito comum vir à mente situações como exposição de dados causadas por ataques de hackers, venda de dados pessoais no mercado, uso malicioso de informação para cometer fraudes etc. O que estes cenários têm em comum é que todos estão sobre o mesmo aspecto do acesso ilegal a dados pessoais, todavia, há uma grande quantidade de dados acessados de forma legal, seja através da coleta de dados entre data brokers que pode ser baseada no consentimento dado pelo titular para a partilha de seus dados ou por outra base legal, como o interesse público (artigo 6 do RGPD).

Autoridades legais têm usado data brokers para conduzir suas investigações por um longo tempo (HOBOKEN; RIEKE; ROBINSON e YU, 2016). Dada a refinada tecnologia de rastreio de dados pessoais capazes revelar entre outros detalhes, comportamentos, gostos e localização de seus titulares e muitas destas informações são geradas em plataformas online como redes sociais e coletadas por data brokers, que acabam por ser umas das fontes de informações de autoridades policiais, havendo nos Estados Unidos data brokers focados em oferecer dados às autoridades (HOBOKEN; RIEKE; ROBINSON e YU, 2016).

Há data brokers nos Estados Unidos que ao invés de fornecerem dados pessoais comercializam ferramentas capazes de manipular tal informação de acordo com os interesses das autoridades como, por exemplo, localização de fugitivos ou outras informações que possam contribuir para a rápida solução

de casos ou diminuição de atividade criminosa (HOBOKEN; RIEKE; ROBINSON e YU, 2016).

Grande parte dos dados processados tem como origem registros públicos que parecem ter um papel maior neste ramo do que para fins de marketing, por exemplo. Estes dados são cruzados com dados de fonte privada com o uso de ferramentas de buscas providenciadas por data brokers como LexisNexis e TransUnion.

O estudo realizado pela Open Society Foundation afirma que o uso de ferramentas de buscas fornecidas por data brokers possui elevados riscos, onde mesmo a menor imprecisão nos dados pessoais pode ocasionar consequências desastrosas ao titular (HOBOKEN; RIEKE; ROBINSON e YU, 2016). Um erro pode levar à uma abordagem mais agressiva de uma pessoa se a informação equivocada classificá-la como perigosa ou como suspeita de uma atividade criminosa, correndo ainda o risco de aprisionamento injusto.

Na mesma esteira, autoridades legais podem, através de dados fornecidos por data brokers ter acesso a dados pessoais de indivíduos com o intuito de oprimir seus direitos, como direito de expressão, direito à educação etc. Em países em que a homossexualidade é crime, órgãos do sistema de justiça podem perseguir os titulares dos dados com base na informação obtida (número telefônico, endereço, geolocalização etc.)

2.2. Estudo de caso: avaliação de políticas de privacidade

Como demonstrado neste estudo, data brokers acessam dados oriundos de fontes online e offline. Com a sociedade cada vez mais digitalizada maior tem sido interação entre indivíduos e plataformas digitais. Neste sentido, redes sociais têm exercido um grande papel no processamento de dados pessoais e servido como fontes para data brokers, isto porque, como acontece com as

corretoras de dados, estas empresas nem sempre possuem uma clara política de privacidade que permita ao titular ter um entendimento claro sobre o que será feito com seus dados pessoais ou que permitam os usuários controlarem o compartilhamento de seus dados (FORBRUKERRADET, 2020).

Estas empresas coletam uma enorme quantidade de dados pessoais sobre indivíduos ao longo de suas vidas e, como já abordado, a falta de transparência é um dos grandes problemas inerentes ao data brokering. Estas empresas raramente têm como fonte de coleta o titular diretamente, mas sim outras fontes.

O objetivo desta seção é análise da política de privacidade de alguns dos maiores data brokers sob a ótica do RGPD e verificar como a informação a respeito do processamento dos dados pessoais é prestada ao titular.

2.2.1. Equifax

Equifax é um data broker que atua na prestação de serviços de análise de crédito para o setor automotivo, comunicação, serviços financeiros, seguros, e-commerce etc. A política de privacidade que será analisada será relativa à Equifax Iberia, S. L. que atualmente se encontra abrangida pelo RGPD. De acordo com sua política, a empresa faz a recolha dos seguintes dados pessoais (EQUIFAX, 2018):

- a) Dados de identificação: nome, sobrenome;
- b) Dados de contacto: telefone, endereço postal, e-mail;
- c) Detalhes de emprego: empresa a que pertence, setor, cargo;
- d) Transações de bens e serviços: Bens e serviços fornecidos;
- e) Outros: dados de navegação, de acordo com a política de cookies.

Quanto às finalidades do tratamento, estas em sua maioria estão dentro das previstas no artigo 6º do RGPD e permitem ao titular ter a compreensão dos propósitos para os quais seus dados estão sendo recolhidos a recolha se baseia em:

- a) Execução de um contrato;
- b) Interesse legítimo;
- c) Consentimento;
- d) Cumprimento de obrigação legal;
- e) Transferência de dados e transferências internacionais.

É fornecida informação sobre a quem o titular pode requerer que seus dados parem de ser recolhidos, no entanto, apenas no que tange ao interesse legítimo não sendo esclarecido como proceder caso não concorde com as outras finalidades o que indica certa limitação do poder de escolha na qual o data broker parece querer compensar quando informa ao consumidor como pode proceder caso não queira receber propagandas ou promoções quando seus dados são recolhidos tendo como base seu consentimento. Ressalta-se que no que tange a última finalidade, esta se trata de uma combinação entre cumprimento de obrigação legal e interesse legítimo.

A falta de transparência é uma das principais preocupações em volta da atividade dos data brokers, portanto, Equifax não é uma exceção. A empresa falha em informar, por exemplo, quais são as empresas com quem partilha os dados pessoais e apenas indica genericamente a quais setores elas pertencem. Na mesma esteira, a empresa não dá garantias de que após cumprida a finalidade do tratamento os dados serão apagados, pois se refere aos dados recolhidos, mas não indicada se isto se aplica apenas aos dados recolhidos por ela ou através dela para terceiros. Isto porque como informado pelo próprio data broker “A EQUIFAX não controla o conteúdo, as políticas de privacidade ou as práticas dos sites de terceiros ou assume qualquer responsabilidade por eles” (EQUIFAX, 2018).

A generalidade relativa a destruição dos dados pessoais após as finalidades da recolha serem atingidas gera a problemática relacionada a extensão desta destruição, pois ao que parece ela se dá apenas a nível externo, ou seja, depois que o data broker concluir que as finalidades foram alcançadas irá proceder com a destruição dos dados depois de certo tempo, todavia, não garante que os terceiros com quem os partilhou farão o mesmo, até porque pode nem ter conhecimento das finalidades que estes terceiros têm bem como as dos demais com os quais estes eventualmente partilharam os dados. Outro problema identificado é o da aparente limitação do direito ao apagamento dos dados que será feito “sempre que possível” (EQUIFAX, 2018). O Considerando 65 do RGPD aduz que²⁵:

Os titulares dos dados deverão ter direito a que os dados que lhes digam respeito sejam retificados e o «direito a serem esquecidos» quando a conservação desses dados violar o presente regulamento ou o direito da União ou dos Estados-Membros aplicável ao responsável pelo tratamento. Em especial, os titulares de dados deverão ter direito a que os seus dados pessoais sejam apagados e deixem de ser objeto de tratamento se deixarem de ser necessários para a finalidade para a qual foram recolhidos ou tratados, se os titulares dos dados retirarem o seu consentimento ou se opuserem ao tratamento de dados pessoais que lhes digam respeito ou se o tratamento dos seus dados pessoais não respeitar o disposto no presente regulamento (...).

²⁵ Disponível em WWW:<URL <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679#d1e2479-1-1>

O direito ao apagamento dos dados é uma consequência direta do princípio da exatidão titulado no artigo 5º do Regulamento, todavia, ao que a política de privacidade da Equifax indica, este direito é limitado e o data broker não informa os casos nos quais o apagamento não será possível, o que é incompatível com dois dos princípios do RGPD. Soma-se ainda o fato de que a empresa deixa completamente ao cargo do titular buscar por eventuais atualizações da sua política de privacidade, pois somente torna disponível quando isto ocorre através de um aviso informativo em seu website, ou seja, no caso do titular estiver ciente de que seus dados estão sendo processados, deverá ter de verificar pessoalmente por atualizações.

2.2.2. Oracle

Ao lado da Equifax, o data borker Oracle exerce um grande papel no mercado de dados o oferece diversas soluções voltadas para os setores de energia, retalho, comunicações, saúde etc. Da mesma forma que o data broker anterior, Oracle recolhe dados pessoais baseados no interesse legítimo, execução de contrato, consentimento e obrigação legal (ORACLE, 2022).

É expectável que, como ocorre com a maioria dos data brokers, a recolha de dados pessoais se dê de forma indireta e não haja muita informação sobre como esse processo é feito. Oracle se mostra fiel a este fato tendo em conta que há limitada informação a esse respeito em sua política. De acordo com o broker, os dados são processados para fins empresariais e comerciais, todavia, é difícil perceber a total dimensão do processamento. Tendo em vista o processamento dos dados para fins de marketing, a empresa usa da informação para enviar propaganda direcionada sobre produtos e serviços e permite que terceiros com quem partilhou os dados façam o mesmo. A

possibilidade de exercer o direito ao apagamento ou correção de erros não é informada de forma transparente, uma vez que o link disponibilizado para o preenchimento da requisição não informa, por exemplo, prazo de resposta e nem a extensão para o exercício dos direitos.

Outro fato notado é o de que o data broker não esclarece quem são os terceiros com quem compartilha os dados coletados o que poderia ao menos permitir ao titular tentar requisitar destas empresas informações referentes a finalidade do processamento, base legal e outros direitos previstos no artigo 15 do RGPD. O referido artigo aduz que²⁶:

1. O titular tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e as seguintes informações:

- a) As finalidades do tratamento;
- b) As categorias dos dados pessoais em questão;
- c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais;
- d) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais que diz respeito ao titular dos dados, ou o direito de se opor a esse tratamento (...)

²⁶ Disponível em WWW:<URL <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679#d1e2479-1-1>>

O data broker se exime de quaisquer responsabilidade no que tange ao tratamento dos dados pessoais por terceiros, todavia, compartilha e recolhe dados com estes sem tornar público ao titular que terceiros são estes o que constitui uma violação do seu direito, pois, como poderá corrigir um dado inexato se não sabe quem foi o responsável por tal inexatidão? O Regulamento prevê que a responsabilidade em caso de danos causados pelo tratamento é, em regra, solidária e que a exceção se limita a comprovação pelo responsável pelo tratamento de que não contribuiu com a origem do dano (artigo 82, RGPD). Todavia, como demonstrado a falta de transparência e a recolha excessiva de dados são vertentes comuns na atividade dos data brokers, logo, pode-se concluir que todos vão ser solidariamente responsáveis por danos, mesmo no caso onde a origem do dano foi um terceiro, aquele que compartilhou os dados com estes também seria responsabilizado tem o dever de verificar se o terceiro segue as determinações do Regulamento, o que Oracle informa fazer sendo assim, solidariamente responsável por eventuais danos oriundos do tratamento de dados pessoais.

2.2.3. Experian

A empresa atua no fornecimento de dados a respeito de consumidores com foco principal ao setor de marketing, mas também para outros setores como financeiro, seguros, entretenimento etc. Em seu site, há várias políticas voltadas para os diferentes setores nos quais atua e, de acordo com sua

política de privacidade de marketing, o broker processa, entre outros, os seguintes dados pessoais²⁷:

- a) Demografia — idade, sexo, estado civil, renda, ocupação e educação
- b) Comportamento e estilo de vida — hobbies, atividades esportivas, preferências de viagem, usuários de equipamentos de alta tecnologia e comportamento de compra
- c) Censo — idade média, classificação de riqueza e renda mediana
- d) Imóveis — informações dos registros de propriedade locais, como tipo de unidade de habitação, preço de compra, valor da hipoteca, tipo e data do empréstimo, juros prevalecentes no momento da venda e características da propriedade
- e) Eventos da vida — consumidores que se mudaram ou compraram uma casa recentemente
- f) Interesses on-line — informações sobre categorias de interesses do consumidor derivadas do uso on-line

Ao analisar a política de privacidade da Experian Marketing, não foi possível verificar nenhuma informação referente a base legal para o tratamento dos dados pessoais que, como se pode observar pela lista acima, abrangem uma parte significativa da vida do titular, ainda mais quando se soma à esta lista o fato de que o broker separa os titulares do dados em categorias como

²⁷ Disponível em [WWW<:URLhttps://www.experian.com/privacy/marketing-data-practices-and-policies>](https://www.experian.com/privacy/marketing-data-practices-and-policies)

consumidores individuais e famílias onde processa e classifica informações relacionadas como renda, nível de educação, interesses etc. (EXPERIAN, 2018).

Há uma política dedicada em informar o consumidor sobre como os dados pessoais são tratados, todavia, embora mais abrangente que a política de marketing, pois informa as finalidades para o tratamento, não esclarece em uma linguagem clara qual é a base legal do tratamento o que se infere que sejam duas: o consentimento e obrigação legal. Na mesma linha, não é possível saber o tempo no qual os dados serão processados, qual o procedimento a ser adotado uma vez que as finalidades forem cumpridas nem mesmo quais são os direitos do titular dos dados pessoais além de um genérico direito de exclusão de dados.

2.2.4. Conclusão

Com a análise da política de privacidade de três grandes data brokers é perceptível a incompatibilidade da sua atividade com o RGPD. O que fica evidenciado é que os três falham em prestar a informação de forma clara ao titular sobre o tratamento de seus dados e há apenas um número limitado de recursos que permitem com um indivíduo possa exercer seus direitos previstos no Regulamento como, por exemplo, correção de dados inexatos, apagamento de dados ou de ter ciência de quem está processando seus dados.

Seguir o caminho do compartilhamento dos dados pessoais é algo extremamente difícil com base nas políticas analisadas. Nenhum dos brokers oferece de forma clara informações sobre como o titular pode exercer seus direitos quando seus dados são compartilhados com terceiros, em que pese

alguns mencionarem com quem compartilham os dados, nem sempre possibilitam uma ligação direta aos mesmos.

Em geral, o titular que tem seus dados pessoais processados por estes brokers se encontram em uma situação de extremo desequilíbrio, pois estas empresas detêm uma enorme e precisa quantidade de dados sobre suas vidas e na maioria das vezes, sem o seu conhecimento e, mesmo que o titular tente entender como seus dados estão sendo tratados se depara como uma escassez de informação.

3. FRAMEWORK LEGAL: LEGISLAÇÃO E DAS DECISÕES DAS AUTORIDADES DE CONTROLE. ANÁLISE JURÍDICA DA ATIVIDADE DOS DATA BROKERS

3.1. REGULAMENTO DE GOVERNAÇÃO DE DADOS

O Regulamento da Governação de Dados (RGD) tem como intuito a harmonização da partilha de dados pessoais e o desenvolvimento de um mercado interno seguro promovendo a cooperação entre os Estados-Membros da União Europeia (Regulamento (UE) 2022/868). Tal instrumento jurídico tem enfoque na reutilização de dados públicos, recolhidos por entidades do setor público bem como incentiva os Estados-Membros a criarem e disponibilizarem dados em conformidade com o princípio “Abertos desde a conceção e por defeito” do artigo 5º, 2 da Diretiva (UE) 2019/1024²⁸.

²⁸ “Os Estados-Membros incentivam os organismos do setor público e as empresas públicas a produzir e disponibilizar documentos abrangidos pelo âmbito de aplicação da presente diretiva em conformidade com o princípio «abertos desde a conceção e por defeito».” Disponível em WWW:<<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019L1024&from=en>>. Acessado em 23.05.2023

De forma concisa e detalhada, este mecanismo jurídico configura as regras para o processamento de dados pessoais e põe todo o controle nas mãos dos Estados, quer seja para regular ou ajudar intermediadores de dados com o processamento. O tratamento dos dados tem como requisito essencial a existência de um ambiente tratamento seguro. De acordo com o artigo 2º, 20 do RGD, ambiente de tratamento seguro é²⁹:

(...) o ambiente físico ou virtual e os meios organizacionais destinados a assegurar o cumprimento do direito da União, tal como o Regulamento (UE) 2016/679, em especial no que respeita aos direitos dos titulares dos dados, os direitos de propriedade intelectual, a confidencialidade comercial e estatística, a integridade e a acessibilidade, bem como o cumprimento do direito nacional aplicável e permitir à entidade que fornece o ambiente de tratamento seguro determinar e supervisionar todas as ações de tratamento de dados, incluindo a visualização, o armazenamento, o descarregamento e a exportação de dados, bem como o cálculo de dados derivados através de algoritmos computacionais;

Outra característica para o processamento de dados é que este deve ter somente fins não comerciais ou de investigação científica, sendo excluídos aqueles que agregam valor aos dados pessoais, como é o caso dos data brokers. Toda a ideia em volta do RGD é de propagar a colaboração entre

²⁹ Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32022R0868>

Estados-Membros e permitir inovação tecnológica a partir do processamento de dados pessoais por entidades públicas ou prestadores de serviços de intermediação de dados supervisionados pelos Estados.

Assim como ocorre com o RGPD, O RGD também prevê a recolha de dados pessoais com base no consentimento e prega a transparência no seu tratamento. Com relação à transparência, nota-se que há um maior esforço para garantir a sua observância como, por exemplo, o fato de ser conhecido quem são as entidades responsáveis pela execução do tratamento assim como com o artigo 3º,1 determinando que a decisão de concessão ou recusa deve ser tornada pública. O mesmo artigo determina ainda a anonimização dos dados a serem reutilizados como condição para o tratamento, uma das medidas organizacionais defendidas para a garantia da segurança no processamento.

Importante ressaltar que o consentimento exerce um papel fundamental no tratamento de dados pessoais no setor público. O artigo 12º, m do RGD determina que os prestadores de serviços de intermediação atuem de forma a garantir o melhor interesse dos titulares dos dados, prestando informações e aconselhamento de forma transparente e clara. Na mesma esteira, as organizações de altruísmo que disponibilizam dados de forma voluntária devem agir expressamente a partir do consentimento dado pelos titulares (Regulamento (UE) 2022/868).

Não se pode negar que o RGD é um instrumento de grande valia no que tange ao processamento de dados pessoais e dá muito mais ênfase a como o processo deve ser executado ao estabelecer regras e limitações assemelhando-se com o RGPD ao defender a transparência, o consentimento e a segurança no tratamento dos dados pessoais e é ainda mais assertivo nestes aspectos. Todavia, por normatizar um segmento específico que é a reutilização de dados pessoais por setores públicos, é quase totalmente incompatível com a atividade dos data brokers.

Diferentemente do que ocorre com o RGPD onde há margem para atuação dos data brokers, o RGD é categórico ao determinar que o processamento dos dados não pode ter fins comerciais e agregar valor aos dados pessoais é o cerne do data brokering. A reutilização de dados não exclui a possibilidade de ter lucros e isto está previsto no artigo 6º deste Regulamento que trata das taxas referentes ao processamento, todavia em uma escala totalmente diferente daquilo que é a atividade dos data brokers que é voltada majoritariamente para a maior obtenção de lucros possível a partir da comercialização dos dados.

Outro ponto que o RGPD se difere do RGD é que este estabelece prazos para o tratamento dos dados (artigos 4º, 9º), e como discutido anteriormente, o RGPD não traça limites claros para, por exemplo, a extensão do consentimento fornecido ou por quanto tempo o processamento deve ser realizado, enquanto uma limitação temporal somente está presente no RGPD no que diz respeito aos subcontratantes. Esta lacuna temporal se mostra favorável aos data brokers, pois processar dados por mais tempo do que alguns meses ou um ano é muito mais vantajoso.

A transparência no processamento de dados pessoais no RGD é estabelecida de forma muito mais estruturada do que no RGPD ao determinar a existência de pontos de informação únicos para esclarecimentos das condições para reutilização dos dados e as taxas relevantes (Regulamento (UE) 2022/868) e notificação por parte daqueles que tencionem prestar serviços de intermediação de dados em um dos Estados-Membros que devem ter ao menos uma autoridade competente para receber tais notificações e decidir sobre a concessão ou não da autorização para o processamento.

Como observado, a falta de transparência é uma característica dos data brokers que se mostra presente desde a primeira etapa do seu modelo de negócio. O nível de controle que os Estados-Membros possuem quanto a

reutilização de dados por entidades públicas ou as expensas do orçamento público não está presente no RGPD e por esta razão data brokers têm muito mais liberdade de atuação, o que não deveria ocorrer tendo em vista os princípios defendidos pelo Regulamento.

Há ainda de se levar em consideração que o RGPD trata apenas de dados públicos e majoritariamente já tratados por entidades públicas. Tendo em vista que os dados coletados por data brokers podem ser oriundos de fontes públicas, pouco parece que os dados abrangidos por este instrumento jurídico seriam tratados pelos brokers que teriam que se submeter ao rigoroso controle do RGPD.

3.2. DIRETRIZES 05/2020 RELATIVAS AO CONSENTIMENTO NA AÇÃO DO REGULAMENTO 2016/679

O presente instrumento jurídico faz uma análise do conceito de consentimento para o processamento de dados pessoais referido no RGPD e enfatiza que os requisitos para o consentimento “não são considerados um ‘dever suplementar’, são antes condições prévias para o tratamento lícito” (DIRETRIZES 05/2020).

A sessão número 3 da Diretriz trata dos elementos necessários para a manifestação do consentimento lícito nos moldes do que prega o artigo 4º, 11 do RGPD, que deve ser: livre, específica, informada e explícita. Quanto ao primeiro elemento, afirma que o titular deve ter a liberdade para consentir e que o consentimento não lhe deve ser imposto no sentido de sofrer as consequências por não o dar, situação já anteriormente mencionada neste trabalho com relação ao fato de que se o titular não consentir com a políticas de privacidade de determinado domínio ou aplicação, não terá acesso aos mesmos, o que contraria a Diretriz e, portanto, o RGPD.

O dispositivo traz à baila a condicionalidade para o consentimento que se dá nos casos de uma aceitação de condições gerais de um contrato ou condicionar a sua execução ao consentimento para o tratamento dos dados pessoais (DIRETRIZES 05/2020), o que vai na contramão do consentimento livre. É defendido que a finalidade para o tratamento não seja uma contrapartida para a realização de um contrato ou prestação de serviço e que estes dois fundamentos do consentimento, consentimento e contrato, não devem se misturar. Para este entendimento, é apresentada uma exceção que ocorre quando o responsável pelo tratamento dá a liberdade para o titular optar por usufruir de um serviço ou, firmar um contrato onde os dados pessoais serão tratados para fins complementares ou, optar por um serviço ou contrato de mesma natureza em que os dados também serão tratados para fins complementares onde o consentimento não é requerido. A Diretriz afirma que³⁰:

(...) Desde que haja a possibilidade de o contrato ser executado ou de o serviço contratado ser prestado por esse responsável pelo tratamento sem consentimento para uma outra utilização dos dados ou para a utilização complementar em causa, significa isto que deixa de existir um serviço sujeito a condicionalidade. (...)

Noutra esteira, é apresentado o conceito de granularidade no tratamento de dados pessoais, ou seja, o consentimento deve ser em relação a uma finalidade específica, se o pedido feito para o processamento tiver finalidades

³⁰ Disponível em [WWW<:URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf>](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf)

distintas, é necessário que haja consentimento para cada uma separadamente, caso contrário, este não será lícito. Isto se traduz, por exemplo, se uma empresa ou broker pedir o consentimento para tratar os dados pessoais do titular, não pode incluir no mesmo pedido a previsão de compartilhamento com terceiros (DIRETRIZES 05/2020) todavia, como explanado anteriormente o compartilhamento de dados faz parte da atividade dos data brokers, quer seja na origem da coleta através de outros brokers ou demais fontes onde o contato com o titular não é direto ou, uma vez tratados e classificados, na comercialização da informação com empresas ou outros brokers para fins diversos. Tal compartilhamento nem sempre se dá sob a égide do consentimento, uma vez que o titular pode nem sequer está ciente do tratamento.

Quanto ao consentimento específico, este também deve ser observado em conjunto com a granularidade no sentido de o responsável pelo tratamento aplicar³¹:

- i especificação em função da finalidade como salvaguarda contra o desvirtuamento da função,
- ii granularidade nos pedidos de consentimento, e
- iii separação clara entre as informações relacionadas com a obtenção de consentimento para atividades de tratamento de dados e as informações sobre outras questões.

³¹ Disponível em [WWW<:URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf>](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf)

Para cada pedido de consentimento, os titulares devem ter informações específicas sobre quais dados serão tratados e suas finalidades os permitindo assim, dá o consentimento específico para o processamento.

Em relação ao consentimento informado, a Diretriz reforça que o titular dos dados pessoais tem o direito de acesso à informação antes de dá o seu consentimento para o tratamento e que esta informação deve ser acessível sob pena ser inválido (DIRETRIZES 05/2020). Tendo em vista este elemento do consentimento, em caso de compartilhamento entre terceiros com base no consentimento original, o terceiro deve ser identificado. Este é um fator de extrema valia para garantir a transparência na atividade dos dados brokers, uma vez que deveriam tornar pública a sua identidade aos titulares dos dados quando da coleta baseada no consentimento.

O consentimento explícito é necessário quando há um risco maior para a proteção dos dados pessoais (DIRETRIZES 05/2020). O RGPD prevê a sua expressa observância no artigo 9º que trata das categorias especiais de dados (raça, crenças religiosas ou filosóficas, opiniões políticas etc.) A Diretriz enfatiza a importância do titular explicitamente com o tratamento de seus dados pessoais, o que poderia ser garantido, mas não exclusivamente, através de uma declaração escrita.

Um cenário trazido pelo instrumento jurídico é o da verificação do consentimento em duas fases em que o responsável pelo tratamento ao ter acesso a um banco de dados que possui informações pessoais sobre o titular, o comunica e informa que tem a intenção de processá-los e, se o titular permitir o tratamento poderá preencher um formulário no que dá o seu consentimento expresso. Isto poderia ser aplicado nos casos de compartilhamento de dados pessoais entre terceiros onde houvesse dúvida se o “consentimento original”, ou seja, dado na primeira coleta, é válido ou não para o compartilhamento.

Como é possível perceber, o consentimento é um dos requisitos fundamentais para a garantia da licitude no processamento de dados pessoais sendo uma das principais bases legais para a atividade dos data brokers quer seja quando têm uma relação direta com o titular no momento da coleta ou, quando do acesso aos mesmos através de compartilhamento entre terceiros onde se presume que em algum momento o consentimento foi dado. Entretanto, é sabido que na vasta maioria dos casos o processamento pode se dá sem a ciência do titular sobre o mesmo, o que como demonstrado, é totalmente contra os princípios defendidos no RGPD.

Em que pese a presente Diretriz explicar como o consentimento dado pelo titular para o processamento dos dados pessoais deve ocorrer para garantir a licitude do tratamento, abrangendo cenários como um consentimento dado em duas fases ou reforçando que para cada finalidade um consentimento específico é necessário, ainda há uma lacuna a qual os data brokers exploram que é falta de um procedimento para a garantia do cumprimento das determinações do RGPD. Sabe-se que as Diretrizes não têm poder vinculativo, mas como um guia para a aplicação do Regulamento, são um instrumento importante no framework legal relativo ao processamento dos dados pessoais e para evidenciar a incompatibilidade da atividade dos data brokers com as atuais normas e como a sua regulação é necessária para a garantia da proteção dos direitos dos titulares.

3.3. PROPOSTA DE REGULAMENTO RELATIVO À PRIVACIDADE E ÀS COMUNICAÇÕES ELETRÔNICAS (DOCUMENTO 52017PC0010)

A proposta que irá substituir o atual Regulamento de Privacidade também conhecido como Lei Europeia de Cookies ou e-Privacy (Diretiva 2002/58/CE) era suposta entrar em vigor em 2018, o que ainda não aconteceu (PRIVACY,

2022). O novo Regulamento traz regras mais firmes que irão impactar de forma significativa empresas que coletam ou processam dados pessoais a partir de Cookies para fins de propaganda direta, o que naturalmente inclui data brokers.

O Considerando 15 da proposta determina que todos os dados das comunicações eletrônicas com base em cookies são confidenciais, e que seu compartilhamento sem o consentimento do titular, ou partes comunicantes, é proibido (Documento 52017PC0010) Por sua vez, o Considerando 18 afirma que o consentimento prestado deve ser uma escolha verdadeira, livre e com a possibilidade de retirado pelo titular sem ser prejudicado, assim como determina o RGPD e mencionado pelas Diretrizes anteriormente estudadas, enquanto o novo e-Privacy trata do consentimento no seu artigo 9º.

Um fato notório que é mencionado no Considerando 22 é o de que as escolhas relativas as predefinições gerais de privacidade determinadas pelo titular feitas quando fornece o seu consentimento, são vinculativas e se aplicam a terceiros. Isto quer dizer, considerando que os cookies são umas das fontes nas quais data brokers coletam dados, esta coleta deve obedecer às escolhas feitas pelo titular quando consentiu que seus dados forcem armazenados. Esta escolha vincularia os data brokers e as suas finalidades para o processamento de dados, ainda que não fosse estabelecida uma relação direta com o titular.

Configurar cookies antes de ter sido obtido consentimento será proibido uma vez que o instrumento legal entrar em vigor. Antes do armazenamento dos dados do consumidor, os domínios (sítios) deverão fornecer ferramentas que possibilitem um “ato positivo inequívoco a manifestar o acordo livre, específico, informado e explícito (...)” (Considerando 24, do Documento 52017PC0010).

Outro aspecto importante previsto no dispositivo é que o titular exerce um grande poder no controle de seus dados. O novo e-Privacy determina que se

consentirem que seus dados sejam incluídos em uma lista (que contém informações pessoais) os titulares podem determinar as categorias de dados que serão incluídos e por ventura processados, sendo obrigatório informar qual a finalidade das listas antes da coleta dos dados, o que reforça o entendimento que o RGPD tem de para cada finalidade deve haver um consentimento específico, caso contrário o processamento seria ilícito e, o mesmo ocorre no cenário de mudança na finalidade do tratamento sem o consentimento do titular dos dados pessoais.

O direito à privacidade e o princípio da transparência defendido no RGPD se revelam peças fundamentais para o consentimento tratado no novo e-Privacy que defende que diferentes graus de invasão de privacidade sejam equiparados ao mesmo grau de violação. Percebe-se que o novo instrumento eleva o poder que o titular tem sobre como seus dados serão processados ao estabelecer de forma sólida, os procedimentos para a recolha das informações. A atual Diretiva relativa à privacidade das comunicações, em vigor desde 2002 já não se adequa mais a realidade dos tempos atuais de uma sociedade cada vez mais globalizada e digital, onde dados pessoais se tornaram uma valiosa commodity e há uma emergência cada vez maior de proteção do titular, quer seja à sua privacidade ou de outros direitos fundamentais.

A nova normativa irá impactar a atividade dos brokers já desde a sua primeira fase, pois a margem para que coleta de dados oriundos de cookies tenha uma finalidade diferente da determinada inicialmente pelo titular quando concorda em dá o seu consentimento será muito pequena, conforme determina o Considerando 21 e o artigo 13 do novo e-Privacy. A transparência assegurada através da imposição do consentimento de forma clara e estruturada, será uma ferramenta valiosa para trazer à luz data brokers que tem os cookies como uma preciosa fonte de dados online. O impacto não se limitará apenas à primeira etapa, mas alcançará todas as

demais que deverão obedecer às finalidades estabelecidas/concordadas pelo titular quando do consentimento prestado o que, naturalmente, inclui a comercialização dos dados para fins de marketing direto.

3.4. DIRETIVA 93/13 RELATIVA ÀS CLÁUSULAS ABUSIVAS NOS CONTRATOS CELEBRADOS COM OS CONSUMIDORES

Considerando que quando o consentimento para o processamento dos dados pessoais é dado pelo titular de forma livre e não condicionada, a relação criada entre o broker (prestador do serviço) e o titular/consumidor, poderia ser vista sobre a égide da relação de consumo.

O artigo 3º da Diretiva 93/13 defende que uma cláusula na qual não é possível ou não foi objeto de negociação é abusiva. Quanto à negociação, o dispositivo legal afirma³²:

Considera-se que uma cláusula não foi objecto de negociação individual sempre que a mesma tenha sido redigida previamente e, consequentemente, o consumidor não tenha podido influir no seu conteúdo, em especial no âmbito de um contrato de adesão.

O facto de alguns elementos de uma cláusula ou uma cláusula isolada terem sido objecto de negociação individual não exclui a aplicação do presente artigo ao resto de um contrato se a apreciação global revelar que, apesar disso, se trata de um contrato de adesão.

³² Disponível em WWW:<URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31993L0013>>

As políticas de privacidade são a forma mais usual para obtenção do consentimento por parte dos titulares (DUROVIC; MONTANARO, 2021), onde os consumidores podem consentir com um simples click ao acessar um domínio. Tal gesto acarretaria na aceitação dos termos contratuais apresentados pelo site ou aplicação tal como uma assinatura manual de um contrato (RADIN, 2013). Desta forma, políticas de privacidade nas quais o titular não negociou seus termos nem tem a possibilidade para tal, à luz do artigo 3º da Diretiva 93/13, seriam consideradas abusivas. Todavia, como já abordado no presente estudo, nem sempre o consumidor irá ler os termos das políticas de privacidade o que pode ser dá por diversos motivos como serem demasiadamente extensas, terem termos que não sejam totalmente claros aos olhos e capacidades do leitor ou, simplesmente pela falta de entendimento do consumidor da importância dos seus dados pessoais. Diante deste cenário, o consentimento dado não poderia ser levado como genuíno, pois não foram dedicados os esforços necessários para a sua aceitação por parte do titular (RADIN, 2013). Logo, poderia haver uma necessidade de implementação de mecanismos que garantem a publicidade do processamento dos dados pessoais para relembrar o titular como, por exemplo, da revisão periódica do consentimento (BARBOSA, 2022).

O artigo 5º da Diretiva, tal como o RGPD determina que a linguagem apresentada seja clara e compreensível, que possibilite um consentimento esclarecido por parte do titular, todavia, como aponta Margaret Radin, a problemática surge quando o RGPD determina que se tais termos forem observados e o consentimento for dado, ele seria válido mesmo se o consumidor não teve o poder de negociar suas cláusulas como defende a Diretiva em questão (RADIN, 2013).

Sendo a autonomia privada das partes e a liberdade contratual que decorre da mesma pilares do direito contratual (MIYAZATO, 2020), é pressuposto que

o titular é livre para aceitar ou recusar os termos do processamento de dados. Para Inês Lopes (2022) a exigência de uma liberdade irrestrita seria utópica, pois traria como consequência a inexistência de qualquer consentimento válido. Sob a perspectiva da lei geral de contratos portuguesa, o titular é livre para a celebração do contrato, ou seja, aceitar os termos das políticas de privacidade ou cookies ao passo que eventual modificação dos seus termos ou finalidades só é válida diante do consentimento das partes (artigos 405 e 406 do Código Civil Português). Percebe-se que este entendimento se alinha com aquilo que prega o RGPD e a Diretiva.

Considerando dados pessoais como um produto, antes de qualquer transação/processamento, o responsável por tal deve identificar e mitigar os riscos inerentes a atividade que possam a tornar insegura e informar o titular/consumidor sobre o processamento, permitindo que o consumidor decida se aceita ou não o processamento e que tenha ainda a capacidade de optar por retirar seu consentimento (CAJAL, 2022). A garantia da conservação do poder do titular sobre seus dados é muito mais visível na Diretiva do que no RGPD, daí este ser um importante instrumento jurídico para suprir a falta de regulação da atividade dos data brokers.

Aos olhos do RGPD, não parece que a “imperícia” do titular em fornecer o seu consentimento o tornaria inválido uma vez que o pedido seja apresentado de forma transparente, lícita e em linguagem clara. Considerando o escopo do Regulamento de garantir maior proteção aos titulares de dados pessoais, tal determinação de consentimento válido parece ter um caráter de aplicação muito vago que pode ser usado por data brokers para contornar o Regulamento.

A problemática em torno do consentimento válido parece abrir um leque para diferentes interpretações em torno da atividade dos data brokers que, por um lado, têm o RGPD como uma barreira para sua atividade ao mesmo tempo que nele encontra o solo fértil para suas práticas devido a já mencionada falta

de maior clareza por parte da norma de como a mesma deve ser posta em prática em matérias como o consentimento e a garantia da sua observância. Em caso de eventual discussão a respeito se o consentimento dado pelo consumidor é válido que haja dois entendimentos passíveis de serem aplicados, o do RGPD (mais brando) e o da Diretiva 93/13 (mais restrita). A “grey area” reside em saber em que situação um ou o outro será aplicado. Se tomarmos a relação direta entre titulares de dados pessoais com data brokers como uma relação de consumo, parece que há uma maior margem para aplicação de uma norma mais restritiva que é a Diretiva, todavia, este não é um entendimento pacificado uma vez que tal relação vai depender elementos como o tipo de contrato (neste caso, as políticas de privacidade) celebrado entre as partes (SANTOS, 2015).

Sem dúvidas a Diretiva é um grande contributo para a proteção dos titulares de dados pessoais alinhada com o que defende o RGPD na falta de uma legislação específica, aliás, como outras normas tratadas nesta sessão, é dotada de uma aplicação ainda mais restritiva para assegurar os direitos dos consumidores em relação aos data brokers. Quanto à mencionada problemática em torno dos dois cenários para determinar um consentimento válido, parece ser uma matéria na qual os Tribunais e autoridades de controle vão ter que determinar em cada caso em concreto, enquanto não haver uma regulamentação específica para a atividade dos data brokers.

3.4. ENTENDIMENTO DAS AUTORIDADES DE CONTROLE

Um grande instrumento para trazer mais transparência e que poderia ser um aliado da regulação da atividade dos data brokers são as decisões dos Tribunais e autoridades competentes para a fiscalização e garantia do cumprimento do RGPD. A este exemplo, temos a recente decisão do Tribunal

de Primeiro Nível no Reino Unido sobre a Notificação de Execução realizada pelo ICO como resultado da sua investigação tratada no capítulo anterior.

Em 2020, ICO. emitiu uma Notificação à Experian determinando que fossem feitas mudanças nos seus procedimentos relativos ao processamento de dados pessoais, principalmente, a obediência do artigo 14 do RGPD (ICO., 2020). Até que o broker cumprisse a determinação, o processamento de mais de 5 milhões de dados teria de ser suspenso (GATES; TODD, 2023).

Experian apelou da decisão ao mencionado Tribunal que, ao rever a Notificação, decidiu o caso majoritariamente em favor do broker. De acordo com o Tribunal, nos casos de coleta de dados por meio de terceiros, os titulares já tiveram acesso às informações suficientes através de suas políticas de privacidade que estavam relacionadas com o Portal de Informação ao Consumidor da Experian, enquanto que a ICO. alegou que o Portal não era claro o suficiente como determina o artigo 14 do RGPD. Entretanto, o Tribunal concordou com a ICO. no que diz respeito ao de informar 5 milhões de titulares nos moldes do artigo 14 não seria desproporcional e, por isso, a exceção do artigo 14, n. 5 do RGPD não se aplicaria. O fundamento por de trás disto é o de que não notificar tamanha quantidade de titulares tendo como justificativa que isto representaria despesa considerável, não significa que a obrigação é desproporcional, pois, ao verificar o custo relativo ao procedimento, o broker poderia tomar a decisão de não realizar o tratamento dos dados.

O entendimento do Tribunal sobre a exceção prevista do artigo 14, n.5 do RGPD tem um impacto positivo na proteção dos direitos dos titulares, pois é uma exceção que muitos data brokers podem evocar, mas a decisão traz à luz uma relação entre custos de observância da legislação e decisões de negócio. Pode-se entender que, mesmo diante da ciência dos custos relacionados em informar o titular sobre o processamento de seus dados pessoais, e é expectável que data brokers tenham noção dos custos para tal,

o processamento ainda ocorrer, não pode ser alegada a desproporcionalidade para a informação, uma vez que poderia ser decidido simplesmente não continuar com o tratamento. A ICO, ainda estuda se irá apelar da decisão ou não.

Em 2021 a Autoridade Espanhola de Proteção de Dados proferiu uma decisão condenando o data broker Equifax Ibérica a 1 milhão de euros (ONETRUST, 2021). O data broker havia coletado informações financeiras dos titulares reclamantes, sem o seu consentimento e as inseriu no seu bando de dados e, em alguns casos os dados não eram precisos. A autoridade entendeu que o broker não tinha o interesse legítimo para coletar os dados que tinham natureza pública, pois estavam no banco de dados do governo, e que falhou em informar os titulares que estava processando a informação para fins de análises de crédito (STUPP, 2021).

É possível perceber com a decisão da autoridade espanhola que, mesmo em oriundos de fontes públicas, as finalidades para o tratamento dos dados devem permanecer as mesmas estabelecidas desde o início do processamento, como defende o RGPD. Importa ressaltar também que, no caso em específico, os dados estavam nos bancos de dados do governo onde o consentimento do titular pode dar lugar ao interesse público prescrito no artigo 6º do RGPD, ou seja, o broker não poderia justificar o processamento com base no consentimento e nem no alegado interesse legítimo.

Ainda são poucos os casos envolvendo violações ao RGPD por data brokers que resultam em multas ou condenações, o que pode se dar em razão de sua atuação ainda passar despercebida aos olhos dos titulares de dados pessoais e até mesmo das autoridades controladoras. Casos de grande repercussão envolvendo violações ao RGPD geralmente estão associados a grandes empresas de tecnologia como Meta e Amazon que não têm o processamento de dados pessoais como principal razão comercial. Outro fato que é importante destacar é as brechas no RGPD podem ser exploradas por

data brokers e criar casos como o da ICO, que teve decisão parcialmente favorável da Notificação recebida pela autoridade inglesa bem como a decisão da Corte de Apelação romena em março de 2023 de submeter uma série de questões à Corte de Justiça da União Europeia sobre a interpretação do RGPD (JUSTICE, 2023).

CONCLUSÃO

Atualmente, a atividade dos data brokers não está regulada e, comumente, vai de encontro com as determinações do RGPD desde a sua primeira etapa, a da vigilância dos dados.

É possível perceber, com base no presente estudo, que a atividade dos data brokers é incompatível com o RGPD em fatos primordiais como, por exemplo, a transparência. Uma grande parte da atividade dos brokers passa despercebida pelos indivíduos que estão cada vez mais conectados e com acesso à informação, entretenimento etc. que acabam por não perceber a quantidade de dados por eles gerados e que são coletados por empresas como data brokers. Esta incompatibilidade por sua vez, não se traduz em ineficácia.

O RGPD é categórico ao determinar as regras para o processamento dos dados pessoais e, terá como suporte o novo e-Privacy para possibilitar ao titular ter mais controle sobre seus dados pessoais. Na mesma esteira, o direito do consumidor por meio da Diretiva 93/13, mostra-se de grande valia para a proteção do titular na falta de uma norma específica, todavia, o atual framework jurídico parece não ser suficiente para exercer o controle da atividade dos data brokers, pois estes podem encontrar na própria legislação brechas que permitem a sua atuação como, por exemplo, a exceção do artigo 14, n.5 do RGPD referente ao esforço excessivo que envolve informar os titulares sobre o processamento ou, da falta de previsão sobre a extensão do consentimento, bem como a distinção de consentimento válido entre o RGPD e a Diretiva 93/13. Mais do que uma ineficiência, se percebe que o RGPD é insuficiente para tentar regular a atividade dos brokers e que para isto, é necessário haver uma legislação direcionada aliada ao Regulamento e aos demais instrumentos jurídicos para que se possa, assim, alcançar os objetivos nos quais o RGPD foi estabelecido.

REFERÊNCIAS BIBLIOGRÁFICAS

[A]

ALVES – **O que são cookies? Entenda os dados que sites guardam sobre você** [Em linha]. Brasil: Techtudo. [Consult. 22.11.2022]. Disponível em WWW:<URL:<https://www.techtudo.com.br/noticias/2018/10/o-que-sao-cookies-entenda-os-dados-que-os-sites-guardam-sobre-voce.ghml>>.

[B]

BARBOSA, Mafalda Miranda – **Proteção de dados, consentimento e tutela do consumidor** [Em linha]. Portugal: Faculdade de Direito da Universidade de Coimbra. [Consult. 11.06.2023]. Disponível em WWW:<URL:https://www.fd.uc.pt/cdc/pdfs/rev_15_completo.pdf>.

BASHYAKARLA, Varoon; HANKEY, Stephanie; MACINTYRE, Amber; RENNÓ, Raquel and WRIGHT, Gary – **Personal data: political persuasion. Inside the influence industry. How it works.** [Em linha]. Tactical Tech's Data Politics, 2019. [Consult. 05.03.2023]. Disponível em WWW:<URL:<https://cdn.ttc.io/s/tacticaltech.org/Personal-Data-Political-Persuasion-How-it-works.pdf>>.

BERGMANIS-KROATS, Gundars, TWETMAN, Henrik – **Data brokers and security. Risks and vulnerabilities related to commercially available data** [Em linha] Letônia: NATO Strategic Communications Centre of Excellence, 2021. [Consult. 25.09.2022]. Disponível em WWW:<URL:https://stratcomcoe.org/cuploads/pfiles/data_brokers_and_security_20-01-2020.pdf>. ISBN 978-9934.564.31.4.

BIRCKAN, G., DUTRA, M. L., MACÊDO, D. D. J. de, e VIERIA, A. F. G. – **Effects of data protection laws on data brokerage** [Em linha]. Brasil: EAI. [Consult. 12.09.2022]. Disponível em WWW:<URL:<https://eudl.eu/pdf/10.4108/eai.22-7-2020.165673>>.

BRILL, Julie., MCSWEENEY, Terrel., OHLHAUSEN, Maureen K., RAMIREZ, Edith. e WRIGHT, Joshua D. – **Data brokers: a call for transparency and accountability** [Em linha]. Washington, Federal Trade Commission. [Consult. 20.09.2022]. Disponível em WWW:<URL:<https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>>.

[C]

CALIF, Menlo Park – **Meta reports second quarter 2022 results** [Em linha]. São Francisco: Meta. [Consult. 15.11.2022]. Disponível em WWW:<URL:<http://investor.fb.com/releasedetail.cfm?ReleaseID=893395>>.

Carta dos direitos fundamentais da União Europeia (2016). Jornal Oficial da União Europeia (2016/C 202/02). [Consult. 12.09.2022]. Disponível em WWW:<URL:<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR>>.

CIMPANU, Catalin – **49 million user records from US data broker LimeLeads put up for sale online**. [Em linha]. ZDNET. [Consult. 07.03.2023]. Disponível em WWW:<URL: <https://www.zdnet.com/article/49-million-user-records-from-us-data-broker-limeleads-put-up-for-sale-online/>>

CHRISTL, Wolfie. SPIEKERMANN, Sarah – **Networks of control. A report on corporate surveillance, digital tracking, big data & privacy** [Em linha]. Áustria: Facultas, 2016. [Consult. 12.09.2022] Disponível em WWW:<URL:https://crackedlabs.org/dl/Christl_Spiekermann_Networks_Of_Control.pdf>. ISBN 978-3-7089-1473-2.

CHRISTOZOV, Dimitar., TOLEVA-STOIMENOVA, Stefka – **The role of information brokers in knowledge management**. Online Journal of Applied Knowledge Management [Em linha] vol. 7 (2014) p. 114. [Consult.

12.09.2022]. Disponível em WWW:<URL: http://www.iiakm.org/ojakm/articles/2014/volume2_2/OJAKM_Volume2_2pp109-119.pdf>.

COIMBRA, Universidade – **Informação administrativa e proteção de dados: princípios do tratamento de dados** [Em linha]. Coimbra. [Consult. 17.09.2022]. Disponível em WWW:<URL:<https://www.uc.pt/protecao-de-dados/protecao-de-dados-pessoais/principios-do-tratamento-dados>>.

COMMISSION, Federal Trade – **Equifax data breach settlement**. [Em linha]. [Consult. 08.03.2023]. Disponível em WWW:<URL:<https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement#FAQ7>>

CONTENT, Rocket – **Big data: entenda o conceito, suas aplicações em diferentes contextos e como impacta as iniciativas de marketing** [Em linha]. Brasil: Rocket Content. [Consult. 03.10.2022]. Disponível em WWW:<URL:<https://rockcontent.com/br/blog/big-data>>.

CORESIGNAL – **What is a data brokers and why do you need one?** [Em linha]. Nova York: Coresignal. [Consult. 12.09.2022]. Disponível em WWW<URL:<https://coresignal.com/blog/data-broker>>.

[D]

UNICEF – **Declaração Universal dos Direitos Humanos**. [Consult. 13.09.2022]. Disponível em WWW:<URL:<https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>>.

DEIGHTON, John A. e JOHSON, Peter A. – **The value of data: consequences for insight, innovation & efficiency in the U.S. economy**. Harvard Business School. [Consut. 15.11.2022]. Disponível em WWW:<URL: <https://www.ipc.be/~media/documents/public/markets/the-value-of-data-consequences-for-insight-innovation-and-efficiency-in-the-us-economy.pdf>>.

DIJCK, José van, – **Datafication, dataism and dataveillance: big data between scientific paradigm and ideology.** *Surveillance & Society* [Em linha] Amsterdam: Universidade de Amsterdam. [Consult. 17.09.2022]. Disponível em WWW:<URL: <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/datafication/datafic>>.

DIRETIVA 93/13/CEE do Conselho, de 5 de Abril de 1993, **relativa às cláusulas abusivas nos contratos celebrados com os consumidores** [Em linha]. Bruxelas. [Consult. 11.06.2023]. Disponível em WWW:<URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31993L0013>>. Diretiva (UE) 2019/1024 do Parlamento Europeu e do Conselho de 20 de junho de 2019 **relativa aos dados abertos e à reutilização de informações do setor público (reformulação)** [Em linha]. Bruxelas. [Consult. 25.05.2023]. Disponível em WWW:<URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019L1024&from=en>>.

DOCUMENTO 52017PC0010 – **Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas)** [Em linha]. Bruxelas. [Consult. 04.06.2023]. Disponível em WWW:<URL: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52017PC0010>>.

DUROVIC, Mateja; MONTANARO, Marco – **Data protection and data commerce: friends or foes?** [Em linha]. United Kingdom. [Consult. 11.06.2023]. Disponível em WWW:<URL: https://www.researchgate.net/publication/350198599_Data_Protection_and_Data_Commerce_Friends_or_Foes>.

[E]

EXPERIAN – **Privacy policy** [Em linha]. [Consult. 19.03.2023]. Disponível em WWW:<URL:<https://www.experian.com/privacy/marketing-data-practices-and-policies>>

EUROPE, Your – **A proteção de dados ao abrigo do RGPD** [Em linha]. Bruxelas: Comissão Europeia. [Consult. 11.10.2022]. Disponível em WWW:<URL:https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_pt.htm>

EUROPEIA, Comissão – **Como deve ser solicitado o meu consentimento?** [Em linha] Bruxelas: Comissão Europeia. [Consult. 03.10.2022]. Disponível em WWW:<URL:https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/how-should-my-consent-be-requested_pt>.

EUROPEIA, Comissão – **Podem ser recolhidos dados pessoais sobre crianças?** [Em linha]. Bruxelas: Comissão Europeia. [Consult. 05.10.2022]. Disponível em WWW:<URL:https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-personal-data-about-children-be-collected_pt>.

EUROPEIA, Comissão – **What is a data controller or a data processor?** [Em linha]. Bruxelas: European Commission. [Consult. 25.09.2022]. Disponível em WWW:<URL:https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en>.

[F]

FIA – **Data mining: o que é, para que serve e tipos de técnicas** [Em linha]. São Paulo: FIA Business School. [Consult. 12.09.2022]. Disponível em WWW:<URL:<https://fia.com.br/blog/data-mining>>.

FERREIRA, Sergio – **RGPD – 7 princípios fundamentais** [Em linha]. Portugal: Blog SGS Portugal. [Consult. 13.09.2022]. Disponível em WWW:<URL:<https://www.sgs.pt/pt-pt/news/2021/11/rgpd-7-principios-fundamentais>>.

FORBRUKERRADET – **Out of control. How consumers are exploited by the online advertising industry** [Em linha]. [Consult. 12.09.2022]. Disponível em WWW:<URL:<https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf>>

FRAZÃO, Ana – **A indústria dos dados pessoais e os data brokers** [Em linha]. Brasil. [Consult. 20.09.2022]. Disponível em WWW:<URL:<https://minutodaseguranca.blog.br/a-industria-dos-dados-pessoais-e-os-data-brokers>>.

[G]

GATES, Tom; TODD, Elle – **A sigh of relief for data brokers: tribunal overturns (most of) ICO's Experian enforcement notice** [Em linha]. United Kingdom. [Consult. 04.06.2023]. Disponível em WWW:<URL:<https://viewpoints.reedsmith.com/post/102i8l8/a-sigh-of-relief-for-data-brokers-tribunal-overturns-most-of-icos-experian-en>>.

GRIFFITH, Eric. **The worst data breaches in 2022: were you a victim?** [Em linha]. PCMAG. [Consult. 03.03.2023]. Disponível em WWW:<URL:<https://www.pcmag.com/news/cybercrime-in-2022-fewer-data-breaches-but-more-victims>>

CAJAL, Ramon - Algorithmic personalisation of consumer transactions and the limits of contract law [Em linha]. Barcelona: Mirea Artigot Golobardes, 2022. Vol. 1-1. [Consult. 11.06.2023]. Disponível em WWW:<URL:<https://ojs.unito.it/index.php/JLMI/article/view/6672/1-2022-ArtigotGolobardes>>.

[H]

HOBOKEN, Joris von; RIEKE, Aaron; ROBINSON, David e YU, Harlan – **Data brokers in an open society**. [Em linha]. Londres: Open Society Foundation. [Consult. 08.03.2023]. Disponível em WWW:<URL <https://www.opensocietyfoundations.org/uploads/42d529c7-a351-412e-a065-53770cf1d35e/data-brokers-in-an-open-society-20161121.pdf>>

[I]

ICO. – **ICO investigation into data protection compliance in the direct marketing data brokering sector** – organizations using marketing services of data brokers [Em linha]. Londres: Ico. [Consult. 25.09.2022]. Disponível em WWW:<URL:<https://ico.org.uk/for-organisations/organisations-using-marketing-services-of-data-brokers>>.

ICO – **Data Protection act 2018 (part 6, section 149) Enforcement powers of the information commissioner enforcement notice** [Em linha]. Londres. [Consult. 04.06.2023]. Disponível em WWW:<URL: <https://ico.org.uk/media/action-weve-taken/enforcement-notices/2618467/experian-limited-enforcement-report.pdf>>.

[J]

JAMMET, Adiren – **The evolution of EU law on protection of personal data**. European (legal) studies on-line papers, Queen's University Belfast - school of law – Jean Monnet ad personam chair professor D Schiek [Em linha]. Leeds: University of Leeds. [Consult. 12.09.2022]. Disponível em WWW:<URL: <https://ssrn.com/abstract=2501417>>.

JUSTICE, Minister - **Administrative and fiscal litigation** [Em linha]. Bucareste. [Consul. 04.06.2023]. Disponível em WWW:<URL:

https://portal.just.ro/2/SitePages/Dosar.aspx?id_dosar=300000000971773&id_inst=2>.

[L]

LEONG, Dymples e YI-LING, Teo – **Data brokers: a weak link in national security** [Em linha]. The Diplomat. [Consult. 28.02.2023]. Disponível em WWW:<URL: <https://thediplomat.com/2020/08/data-brokers-a-weak-link-in-national-security/>>.

LOPES, Inês Camarinha – **Cláusulas de processamento de dados pessoais inseridas nos contratos de adesão: a falta de autonomia e liberdade na expressão da vontade e vias de proteção (efetiva) do titular de dados** [Em linha]. Espanha: Actualidad Jurídica Iberoamericana No 16, febrero 2022, ISSN: 2386-4567, 2022. [Consult. 11.06.2023]. Disponível em WWW:<URL: <https://revista-aji.com/wp-content/uploads/2022/04/47.-Ines-Camarinha-1124-1147.pdf>>

[M]

MACEDO, Juliana – **Data broker e a LGPD** [Em linha]. Brasil: Diego Castro Advogado. [Consult. 03.10.2022]. Disponível em WWW:<URL:<https://diegocastro.adv.br/coleta-de-dados-por-data-broker-e-a-lgpd/>>.

MENEZES, Daniel Francisco Negão – **A proteção do indivíduo quanto ao tratamento de seus dados pessoais em ambiente digital: um entrave à inovação tecnológica?** [Em linha]. Lisboa: Centro de Investigação de Direito Privado. [Consult. 03.10.2022]. Disponível em WWW:<URL: https://www.cidp.pt/revistas/rjlb/2021/4/2021_04_0251_0277.pdf>.

MIYAZATO, Sheila Keiko Fukigauchi – **A autonomia privada no direito contratual contemporâneo** [Em linha]. São Paulo: Revista Pensamento Jurídico. Vol. 14 N o3, 2020. [Consult. 11.06.2023]

[O]

ONETRUST – **AEPD fines Equifax €1M for GDPR lawfulness, accuracy, and transparency violations** [Em linha]. Spain. [Consult. 04.06.2023]. Disponível em WWW:<URL: <https://www.dataguidance.com/news/spain-aepd-fines-equifax-1m-gdpr-lawfulness-accuracy>>.

ORGANIZATION, The European Consumer – **Access to consumers' data in the digital economy** [Em linha]. Bruxelas, 2019. [Consult. 09.03.2023]. Disponível em WWW:<URL https://www.beuc.eu/sites/default/files/publications/beuc-x-2019-068_european_data_policy.pdf>

ORACLE – **Oracle general privacy policy** [Em linha]. [Consul em 13.03.2023]. Disponível em WWW:<URL <https://www.oracle.com/legal/privacy/privacy-policy.html#15>>

[P]

PARTY, Data Protection Working – **Opinion 15/2011 on the definition of consent** [Em linha]. Bruxelas: Comissão Europeia. [Consult. 03.10.2022]. Disponível em WWW:<URL:https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf>.

PEREIRA, Laudelina – **Data broker – modelo de negócio baseado na vigilância da sociedade** [Em linha] São Paulo. [Consult- 17.09.2022]. Disponível em WWW:<URL:<https://www.linkedin.com/pulse/data-broker-modelo-de-neg%C3%B3cio-baseado-na-vigil%C3%A2ncia-l-pereira/?originalSubdomain=pt>>.

PRIVACY, Secure – **EU's ePrivacy Regulation: 2022 updates** [Em linha]. Netherlands. [Consult. 04.06.2023]. Disponível em WWW:<ULR: <https://secureprivacy.ai/blog/eu-eprivacy-regulation-2022-updates>>.

PROTECTION, Swedish Authority for Privacy – **Sensitive personal data** [Em linha]. Estocolmo: IMY. [Consult. 12.09.2022]. Disponível em

WWW:<URL:https://www.imy.se/en/individuals/data-protection/introduktion-till-gdpr/what-is-actually-meant-by-personal-data/what-is-meant-by-sensitive-personal-data>.

PYLES, Victor – **Os data brokers e a comercialização dos dados pessoais** [Em linha]. Brasil: Empório do direito.com.br. [Consult. 03.10.2022]. Disponível em WWW:<URL:https://emporiiododireito.com.br/leitura/os-data-brokers-e-a-comercializacao-dos-dados-pessoais>.

[R]

RADIN, Margaret Jane – **The Boilerplate: the fine print, vanishing rights, and the rule of law** [Em linha]. Estados Unidos: Jornal da Universidade de Princeton, 2014.

REGULAMENTO (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, **relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE)** [Em linha]. Bruxelas [Consult. 12.09.2022]. Disponível em WWW:<URL: https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1559280280904&uri=CELEX:32016R0679#d1e1690-1-1>.

REGULAMENTO (UE) 2022/868 do Parlamento Europeu e do Conselho de 30 de maio de 2022 **relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724 (Regulamento Governação de Dados)** [Em linha]. Bruxelas. [Consult. 25.05.2023]. Disponível em WWW:<URL: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32022R0868>.

RODRIGUES, Bruna Luzes Costa – **O marketing direcionado dos data brokers em face do advento da LGPD: estudo sobre a base legal**

aplicável (2020) [Dissertação de mestrado, Universidade do Estado do Rio de Janeiro]. WWW:<URL:https://itsrio.org/wp-content/uploads/2021/03/Bruna-Luzes-Costa-Rodrigues_Marketing-direcionado-e-Data-Brokers_O-MARKETING-DIRECIONADO-DOS-DATA-BROKERS-EM-FACE-DO-ADVENTO-DA-LGPD-ESTUDO-SOBRE-A-BASE-LEGAL-APLICAVEL.pdf>.

[S]

S.L., Equifax Ibérica – **Política de privacidad** [Em linha]. [Consult. 12.03.2023]. Disponível em WWW:<URL https://soluciones.equifax.es/legal/>STUPP, Catherine - **Data scraping in EU Regulators' sights ss Spain srders Equifax to delete information** [Em linha]. Spain. [Consult. 04.06.2023]. Disponível em WWW:<URL: https://www.wsj.com/articles/data-scraping-in-eu-regulators-sights-as-spain-orders-equifax-to-delete-information-11620293400?page=1.

SANTOS, José Augusto Cerqueira dos – A harmonização do direito do consumo. Recentes desenvolvimentos ao nível europeu e nacional [Em linha]. Portugal. [Consult. 11.06.2023]. Disponível em WWW:<URL: https://repositorio-aberto.up.pt/bitstream/10216/83624/2/36934.pdf.

[T]

TECH, Tactical – **Personal data: political persuasion – the guidebook and visual gallery**. [Em linha]. [Consult. 05.03.2023]. Disponível em WWW:<URL https://ourdataourselves.tacticaltech.org/posts/inside-the-influence-industry/>.