FUNDAÇÃO GETULIO VARGAS

ESCOLA DE DIREITO DE SÃO PAULO

GABRIELA TIEMI MORIBE

A proteção de dados pessoais na Secretaria Nacional do Consumidor (2019-2021)

SÃO PAULO

2022

GABRIELA TIEMI MORIBE

A proteção de dados pessoais na Secretaria Nacional do Consumidor (2019-2021)

Dissertação de Mestrado apresentada ao Programa de Mestrado Acadêmico da Escola de Direito de São Paulo da Fundação Getulio Vargas, como requisito para obtenção do título de Mestre em Direito.

Campo do Conhecimento: Instituições do Estado Democrático de Direito e Desenvolvimento Político e Social.

Orientador Prof. Dr. Daniel Wei Liang Wang

SÃO PAULO

2022

Moribe, Gabriela Tiemi.

A proteção de dados pessoais na Secretaria Nacional do Consumidor (2019-2021) / Gabriela Tiemi Moribe. - 2022.

138 f.

Orientador: Daniel Wei Liang Wang.

Dissertação (mestrado) - Fundação Getulio Vargas, Escola de Direito de São Paulo.

1. Proteção de dados. 2. Direito à privacidade. 3. Defesa do consumidor - Legislação. 4. Brasil. [Lei geral de proteção de dados pessoais (2018)]. 5. Brasil. Secretaria Nacional do Consumidor. I. Wang, Daniel Wei Liang. II. Dissertação (mestrado) - Escola de Direito de São Paulo. III. Fundação Getulio Vargas. IV. Título.

CDU 343.45

Ficha Catalográfica elaborada por: Isabele Oliveira dos Santos Garcia CRB SP-010191/O
Biblioteca Karl A. Boedecker da Fundação Getulio Vargas - SP

GABRIELA TIEMI MORIBE

A proteção de dados pessoais na Secretaria Nacional do Consumidor (2019-2021)

Dissertação de Mestrado apresentada ao Programa de Mestrado Acadêmico da Escola de Direito de São Paulo da Fundação Getulio Vargas, como requisito para obtenção do título de Mestre em Direito.

Campo do Conhecimento: Instituições do Estado Democrático de Direito e Desenvolvimento Político e Social.

Data de Aprovação: 27/06/2022.

Banca Examinadora

_____

Prof. Dr. Daniel Wei Liang Wang (Orientador)

_____

Prof. Dr. Carlos Ari Sundfeld

_____

Profa. Dra. Miriam Wimmer

AGRADECIMENTOS

"*It takes a village to raise a child*" é um provérbio que traduz bem o sentimento de gratidão que gostaria de expressar a todos que de alguma forma contribuíram para a conclusão deste trabalho. Por isso, peço "licença poética" para retirar o provérbio da sua acepção original e introduzir aqui os agradecimentos. Tenho certeza de que é preciso de uma comunidade para concluir um mestrado. A despeito de o seu fim ser um título individual, não poderia deixar de reconhecer aquelas pessoas que no âmbito acadêmico ou pessoal contribuíram para que a dissertação pudesse ser concluída.

Em primeiro lugar, gostaria de agradecer ao meu orientador, Professor Daniel Wang, a quem devo muitas (senão todas) as oportunidades acadêmicas que tive desde a graduação. De voluntária em um grupo de pesquisa sobre judicialização da saúde na graduação à defesa da dissertação de mestrado sobre a tutela de dados pessoais, tive a sorte ao longo dessa trajetória de testemunhar a sua generosidade, contar com a sua disponibilidade e me espelhar em seu exemplo. Sou grata ao Daniel pelo equilíbrio que soube manter entre autonomia e orientação durante o desenvolvimento deste trabalho, sopesando com muita sabedoria confiança, crítica e aconselhamento nos momentos certos.

Sou grata ao Professor Carlos Ari Sundfeld e à Professora Miriam Wimmer pela leitura generosa, assim como pelas críticas e comentários pertinentes que colaboraram para o aperfeiçoamento da versão final deste trabalho. Agradeço também à revisora Daniela Georgeto pela revisão textual da dissertação.

Também gostaria de agradecer a todas as professoras e professores do Programa de Mestrado Acadêmico em Direito e Desenvolvimento da FGV Direito SP. Flávia Püschel, José Garcez, Luciana Gross Cunha, Maíra Machado, Marta Machado, Oscar Vilhena e Sergio Mittlaender ministraram disciplinas e conduziram debates em sala de aula que contribuíram para o desenho desta pesquisa. Ainda, sou grata pela contribuição que tiveram para a minha formação acadêmica enquanto pesquisadora, ampliando meus horizontes teóricos, introduzindo novas ferramentas de pesquisa e ensino, assim como criando espaços qualificados e abertos de diálogo.

Não poderia deixar de agradecer também aos colegas do Programa. Compartilhamos a experiência sem precedentes de viver um mestrado durante uma pandemia, tendo a maior parte de nossas remotas. Sou grata aos colegas pelo senso de pertencimento e comunidade do grupo criado

e cultivado entre nós, ainda que fisicamente distantes. Conheci pessoas brilhantes e admiráveis e sinto orgulho em ter compartilhado parte da minha trajetória com eles. Sou grata a todos os comentários e sugestões feitos às versões anteriores do projeto de pesquisa durante as disciplinas de metodologia. Ainda, agradeço aos pesquisadores Guilherme Klafke e Olívia Pasqualeto pela gentileza e abertura em ensinar-nos sobre o uso do software Atlas.ti.

O Programa de Mestrado Acadêmico da FGV foi estruturado para pesquisadores que pudessem idealmente realizá-lo em dedicação exclusiva. A decisão de continuar na advocacia junto com o Mestrado não teria sido possível sem o apoio de gestores e colegas de trabalho. Sou grata ao Renato Leite, Maria Cecilia de Oliveira Gomes, Pedro Ramos, Fernando Bousso, Kelli Angelini, Karen Borges e Mariana Caparelli por terem sido gestores que compraram comigo o desafio de poder me dedicar ao Mestrado junto com o trabalho. Além dos gestores, não poderia deixar de agradecer o apoio das e dos colegas de equipe que foram suporte e interlocutores de pesquisa, como Adriane Loureiro Novaes, Victor Dotti e Sofia Chang.

Agradeço também à minha mãe, Stella, e ao meu pai, Daniel, pelo apoio incomensurável e por terem sempre incentivado a curiosidade, os estudos e a importância da formação acadêmica. À minha irmã, Giulia, eu agradeço por ser porto-seguro para os momentos desafiadores. Também sou grata a todas as minhas amigas e amigos que foram apoio emocional nos últimos dois anos, proporcionando momentos de lazer e descontração que foram cruciais para um equilíbrio entre dedicação acadêmica e pessoal, em especial Ana Paula Silveira, Barbara Abrantes, Camila Del Nero, Eliza Nitzan, Gabriela Magalhães, Giuliana Kowalski, Gustavo Ferreira de Campos, Joana Furquim, Laura Gasparini, Luciana Maselli, Maraisa Cezarino, Mariana Negreiros, Pamela Michelena. Agradeço também ao Rafael Amarante, que foi suporte emocional e psicológico nos últimos dois anos.

Por fim (mas não menos importante), o agradecimento genuíno para o Giulio, meu companheiro de vida, que me apoiou em todas as etapas (e âmbitos) de pesquisar: transcreveu entrevistas, ajudou a encontrar contatos daqueles que gostaria de entrevistar, revisou cada trecho escrito, contribuiu com comentários de melhoria na escrita ou de concatenação de ideias, assumiu tarefas domésticas para compensar a minha exaustão e me acolheu nos momentos desafiadores. Sou grata por tê-lo como melhor amigo, conselheiro, amor e companheiro – não poderia ter escolhido alguém melhor para compartilhar a conquista que é concluir este trabalho.

RESUMO

A expressão “uso indevido de dados” é corriqueiramente utilizada pelo Departamento de Proteção e Defesa do Consumidor (DPDC) da Secretaria Nacional do Consumidor (Senacon) para descrever as condutas que ensejam os procedimentos administrativos instaurados pelo órgão em temas relacionados à proteção de dados pessoais. À medida que a Senacon se engaja na supervisão e fiscalização de condutas relacionadas à privacidade e à tutela de dados pessoais de consumidores, questões como a forma que a Secretaria tem atribuído sentido à expressão “uso indevidos de dados” e mobilizado conceitos jurídicos para interpretar e decidir esses casos se tornam relevantes para entender como o regime jurídico da tutela dos dados pessoais tem sido mobilizado – “em ação” – pela Senacon. A pesquisa analisa 33 notas técnicas públicas relacionadas às averiguações preliminares e processos administrativos conduzidos pela Senacon entre fevereiro de 2019 e julho de 2021 para identificar as palavras-chave que traduzem a “gramática” adotada pelo órgão nos casos de proteção de dados, com o objetivo de compreender como a abordagem da Senacon à proteção de dados pessoais se relaciona com os conceitos, regras e pressupostos normativos advindos da Lei Geral de Proteção de Dados Pessoais (LGPD – Lei 13.709/2018). A pesquisa conclui que, embora exista sobreposição e utilização de conceitos análogos aos da LGPD pela Senacon, a principal diferença entre a abordagem da Secretaria e o paradigma normativo da LGPD (que se fundamenta na garantia de direitos e prerrogativas para o exercício individual da autodeterminação informativa pelos titulares de dados pessoais) se dá pelo fato de a Senacon adotar o pressuposto normativo da vulnerabilidade do consumidor como lente interpretativa nas decisões sobre “usos indevidos de dados”. Essa abordagem protetiva ao consumidor pelo reconhecimento da sua vulnerabilidade no contexto do uso de seus dados pessoais é o que caracteriza a “gramática” adotada pela Secretaria nos casos estudados.

Palavras-chave: proteção de dados pessoais; privacidade; direito do consumidor; Senacon; LGPD.

ABSTRACT

The expression “improper use of data” is routinely used by the Department of Consumer Protection and Defense (DPDC) of the National Consumer Secretariat (Senacon) to describe the conducts that gives rise to administrative procedures instituted by the agency in matters related to the protection of privacy and personal data. As Senacon engages in the supervision and inspection of conducts related to privacy and the protection of personal data of consumers, issues such as how the Secretariat has given meaning to the expression “improper use of data” and mobilized legal concepts to interpret and decide these cases become relevant to understand how the data protection legal regime data has been mobilized – “in action” – by Senacon. The research analyzes 33 technical notes related to preliminary investigations and administrative procedures conducted by Senacon between February 2019 and July 2021 to identify the keywords that translate the “grammar” adopted by the agency in data protection cases and to understand how Senacon's approach to data protection relates to the concepts, rules and normative assumptions arising from the General Law for the Protection of Personal Data (LGPD - Law 13,709/2018). The research concludes that, although there is an overlap and use of concepts similar to those of the LGPD by Senacon, the main difference from the approach and normative paradigm of the LGPD (which is based on the guarantee of rights and prerogatives for the individual exercise of informative self-determination by the holders of personal data) is that Senacon adopts the normative assumption of consumer vulnerability as an interpretive lens in decisions on “improper use of data”. This protective approach to consumers by recognizing their vulnerability in the context of the use of their personal data is what characterizes the “grammar” adopted by the Secretariat in the cases studied.

Keywords: data protection; privacy; consumer protection; Senacon; LGPD.

"*We have then to try to clarify, first, the new technology and, second, the effects this may have on institutions, policies and uses of television. But we have to do this while remembering that the technology will not determine the effects. On the contrary, the new technology is itself a product of a particular social system, and will be developed as an apparently autonomous process of innovation only to the extent that we fail to identify and challenge its real agencies.*"

(Raymond Williams em *Television: Technology and cultural form*, 1974)

LISTA DE SIGLAS E ABREVIATURAS

ACT	Acordo de Cooperação Técnica
ANPD	Autoridade Nacional de Proteção de Dados
Bacen	Banco Central do Brasil
CDC	Código de Defesa do Consumidor (Lei 8.078/1990)
CF/88	Constituição da República Federativa do Brasil de 1988
CGI.br	Comitê Gestor da Internet no Brasil
CNDC	Conselho Nacional de Defesa do Consumidor
CMN	Conselho Monetário Nacional
Denatran	Departamento Nacional de Trânsito
DPDC	Departamento de Proteção e Defesa do Consumidor
ECA	Estatuto da Criança e do Adolescente (Lei 8.069/1990)
EDPB	*European Data Protection Board*
EFF	*Eletronic Frontier Foundation*
FTC	*Federal Trade Commission*
GDPR	*General Data Protection Regulation (Regulation EU 2016/679)*
IDEC	Instituto Brasileiro de Defesa do Consumidor
INSS	Instituto Nacional do Seguro Social
LAI	Lei de Acesso à Informação (Lei 12.527/2011)
LCP	Lei do Cadastro Positivo (Lei 12.414/2011)
LGPD	Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018)
MCI	Marco Civil da Internet (Lei 12.965/2014)
MDB	Movimento Democrático Brasileiro
Mercosul	Mercado Comum do Sul
MJSP	Ministério da Justiça e Segurança Pública
MP	Medida Provisória
MPDFT	Ministério Público do Distrito Federal e Territórios
MPF	Ministério Público Federal
NYAG	*Ney York Attorney General*
OCDE	Organização para a Cooperação e Desenvolvimento Econômico

Procon	Programa de Proteção e Defesa do Consumidor
Senacon	Secretaria Nacional do Consumidor
Sindec	Sistema Nacional de Informações de Defesa do Consumidor
SNDC	Sistema Nacional de Defesa do Consumidor
TAC	Termo de Ajustamento de Conduta
TFD	Teoria Fundamentada em Dados (*grounded-theory*)

SUMÁRIO

INTRODUÇÃO: O TEXTO EM SEU CONTEXTO

Em setembro de 2020, a Lei Geral de Proteção de Dados Pessoais (LGPD) entrou em vigor após dois anos de *vacatio legis* e oito anos de debates legislativos. Trata-se da primeira legislação brasileira a regular, em âmbito federal, de forma específica e com escopo setorialmente transversal[1], o tratamento de dados pessoais por organizações públicas e privadas em meios físicos ou digitais.

O Anteprojeto[2] que nove anos depois daria origem à LGPD foi inicialmente formulado dentro da Secretaria Nacional do Consumidor (Senacon), órgão vinculado ao Ministério da Justiça. Esse Anteprojeto foi escrito "a quatro mãos"[3] por Laura Schertel Mendes, então Coordenadora-Geral de Supervisão e Controle do Departamento de Proteção e Defesa do Consumidor (DPDC) da Senacon, e Danilo Doneda, que foi Coordenador-Geral de Estudos e Monitoramento da mesma Secretaria.

Durante o processo legislativo da LGPD e mesmo após a sua sanção, um dos pontos mais controversos sobre a lei girou em torno da configuração da Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por implementar e fiscalizar o cumprimento da lei no país. O texto aprovado pelo Congresso Nacional em julho de 2018 previa a criação de uma Autoridade sob o regime de autarquia vinculada ao Ministério da Justiça. Essa Autoridade seria dotada de independência administrativa, autonomia financeira e ausência de subordinação hierárquica a seus dirigentes, por meio da previsão de mandatos fixos e estabilidade.

Contudo, em 14 de agosto de 2018, quando da sanção presidencial da LGPD, o ex-Presidente Michel Temer (MDB) vetou integralmente os dispositivos relacionados à ANPD, alegando "inconstitucionalidade do processo legislativo", sob o argumento de usurpação de

[1] Antes da LGPD ser aprovada, já havia regras sobre privacidade e/ou proteção de dados no ordenamento jurídico brasileiro, como o Código de Defesa do Consumidor, a Lei de Acesso à Informação, o Marco Civil da Internet e a Lei do Cadastro Positivo. No entanto, essas normas eram esparsas, setoriais e não uniformes (BIONI et al., 2015, p. 3). E não havia um aparato institucional consolidado para lidar com essas questões, havendo incertezas sobre instâncias administrativas responsáveis pela sua regulamentação ou fiscalização (SIMÃO; MORIBE, 2021).

[2] Trata-se do Anteprojeto de Lei, que tramitaria no Congresso Nacional sob o nº 2.576/2016 (autoria do Poder Executivo), que foi posteriormente apensado ao Projeto de Lei 4.060/2012 (autoria do deputado Milton Monti – PR/SP).

[3] A organização Data Privacy construiu uma linha do tempo a partir de entrevistas com os principais atores do processo legislativo da LGPD, que narra o histórico de debates em torno da construção legislativa da lei, intitulada "Memória da LGPD". Disponível em: https://observatorioprivacidade.com.br/memorias/. Acesso em: 20 fev. 2021.

prerrogativa legislativa, uma vez que a criação da ANPD teria que partir do Poder Executivo, e não do Legislativo[4]. A despeito dos vícios formais, o ex-Presidente teria sinalizado concordância com a constituição do órgão, comprometendo-se a, futuramente, editar norma para a criação da Autoridade (Agência Senado, 2018).

A promessa seria cumprida em 27 de dezembro de 2018, no apagar das luzes de seu mandato, por meio da Medida Provisória 869. Diferentemente da Autoridade desenhada durante o processo legislativo no Congresso Nacional, a ANPD, na configuração da MP, não mais seria constituída sob o regime de autarquia, ficando diretamente vinculada à Presidência da República. Ainda, a Autoridade seria criada sem aumento de despesa, com o aproveitamento de cargos e funções já existentes na Administração Pública Federal. Nesse novo modelo institucional, a ANPD perdia a ausência de subordinação hierárquica ao Poder Executivo e a independência financeira originalmente propostas.

Durante a conversão da MP na Lei 13.853/2019, o Congresso incluiu a possibilidade de transformação da natureza jurídica da ANPD em autarquia da Administração Pública Federal indireta pelo Poder Executivo, no prazo de dois anos da entrada em vigor da estrutura regimental da Autoridade. A despeito da mudança realizada pelo Legislativo, a persistência da falta de autonomia financeira e administrativa da Autoridade, em especial a incerteza em relação à sua independência hierárquica em relação ao Poder Executivo, suscitou críticas por parte da sociedade civil (Coalizão de Direitos na Rede, 2020).

Durante esse período de controvérsia e indefinição sobre o modelo institucional da ANPD, alguns órgãos[5] tomaram a frente na fiscalização de casos envolvendo dados pessoais, preenchendo

[4] Nos termos da exposição de vetos, "os dispositivos incorrem em inconstitucionalidade do processo legislativo, por afronta ao artigo 61, § 1º, II, 'e', cumulado com o artigo 37, XIX da Constituição". A exposição dos vetos está disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Msg/VEP/VEP-451.htm. Acesso em: 23 fev. 2021.

[5] Vale citar o Ministério Público do Distrito Federal e Territórios (MPDFT), que criou, por meio da Portaria Normativa PGJ 539/2018, uma Comissão de Proteção dos Dados Pessoais especializada, cujas atribuições incluíam: "promover e incentivar a proteção dos dados pessoais"; "promover a defesa dos interesses e direitos difusos, coletivos e individuais homogêneos dos titulares dos dados pessoais"; "sugerir diretrizes para uma Política Nacional de Proteção dos Dados Pessoais e Privacidade"; e "promover ações de cooperação com autoridade de proteção de dados pessoais de outros países, de natureza internacional ou transacional". No âmbito da Comissão, hoje denominada Unidade Especial de Proteção de Dados e Inteligência Artificial, o MPDFT conduziu inquéritos civis, propôs ações civis públicas e firmou termos de ajustamento de conduta em casos de grande repercussão relacionados à proteção de dados pessoais. Vale citar também o Conselho Administrativo de Defesa Econômica (Cade), que, embora não estivesse diretamente envolvido em fiscalizações envolvendo o uso de dados pessoais, elaborou, em agosto de 2020, um estudo propondo a incorporação da ANPD à sua estrutura, sob o argumento de que isso aceleraria a

um vácuo deixado pela ausência de criação da Autoridade quando da sanção da lei. Um dos órgãos que exerceu essa atividade com notável protagonismo foi a Secretaria Nacional do Consumidor.

Vale citar que, durante a tramitação do projeto de conversão em lei da MP 869/2018, em abril de 2019, a Senacon publicou a Nota Técnica 04/19[6], na qual manifestou a preocupação de a nova configuração institucional da ANPD "ir de encontro com os interesses dos consumidores", principalmente pela previsão de a Autoridade ser a última instância de interpretação da LGPD[7], nos seguintes termos:

> A nova competência preponderante da ANPD pode colocar em risco o andamento e *enforcement* dos processos administrativos em andamento – sem prejuízo de outros que possam porventura serem instaurados –, motivo pelo qual não faz sentido que a SENACON seja privada de atuar no âmbito de uma matéria que é inerente às suas competências. Mais do que isso, o consumidor brasileiro está num estágio menos avançado em relação à importância e ao valor econômico de sua privacidade e de seus dados se comparado aos consumidores europeus, tornando a aplicação do Código de Defesa do Consumidor (CDC) desejável nesse estágio de nosso desenvolvimento sócio cultural. (2019, p. 1)

A nota técnica evidenciou uma posição institucional dos membros que então compunham a Secretaria de contrariedade em perder espaço de atuação em questões envolvendo a tutela de dados pessoais de consumidores, uma preocupação que, de acordo com a nota técnica, envolvia, em especial, os procedimentos administrativos instaurados pela Secretaria, os quais incluíram casos de grande repercussão nacional, como o escândalo do *Cambridge Analytica*, em que a Secretaria sancionou o Facebook ao pagamento de multa totalizando R$ 6.600.000,00 (seis milhões e seiscentos mil reais) pelo compartilhamento indevido de dados de usuários.

Em 26 de agosto de 2020, o Planalto publicou o Decreto 10.474, detalhando a estrutura regimental da Autoridade Nacional de Proteção de Dados, bem como o seu quadro de funcionários. Em 15 de outubro de 2020, o Presidente Bolsonaro (PL) indicou os cinco nomes que comporiam o quadro de diretores da ANPD. Quatro dias depois, os indicados foram submetidos à sabatina no

operacionalização da Autoridade e economizaria recursos ao governo federal. O estudo está disponível em: https://www.telesintese.com.br/wp-content/uploads/2020/08/Cade-como-ANPD.pdf. Acesso em: 21 fev. 2021.

[6] Nota técnica nº 04/19/GAB-SENACON/SENACON/MJ, Processo nº 08012.001058/2019-61.

[7] Essa atribuição estava prevista na MP 869/2018 e foi confirmada quando da conversão da MP em lei, que é o seguinte dispositivo: "Art. 55-K. A aplicação das sanções previstas nesta Lei **compete exclusivamente à ANPD**, e suas **competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas** de outras entidades ou órgãos da administração pública. Parágrafo único. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e **será o órgão central de interpretação desta Lei** e do estabelecimento de normas e diretrizes para a sua implementação".

Senado Federal e, no mesmo dia, os cinco nomes foram aprovados pela Comissão de Infraestrutura do Senado.

Com a materialização da ANPD, iniciou-se um período em que os membros que então compunham a Senacon e a representavam publicamente em eventos começaram a inflexionar o discurso anteriormente evidenciado na nota técnica de 2019, abandonando a visão anterior de uma Senacon protagonista para uma posição de maior coadjuvância na seara da proteção de dados. Em evento[8] ocorrido em outubro de 2020, o então Diretor do DPDC, Leonardo Albuquerque Marques, relatou que a Secretaria vinha exercendo um papel de "órgão regulador" por uma questão de "dependência da trajetória", tendo atuado em questões relacionadas à privacidade desde o Marco Civil da Internet, promulgado em 2014. Naquela oportunidade, o então Diretor sinalizou a "remodelação de uma Senacon que vinha, até determinado limite, exercendo o papel de órgão regulador para, guardadas agora as devidas proporções, servir mais como órgão mediador", sustentando que o papel da Secretaria lhe parecia "agora muito mais no sentido de intermediar demandas, (...) não só de Procons, mas de quem quer que seja e o interesse do Consumidor, por diversos canais", "exercer o *advocacy* mesmo do consumidor perante a ANPD".

Na mesma ocasião, Leonardo Marques (2020, minuto 14:26) emitiu a seguinte declaração:

> (...) existe ali um limite do qual a Senacon não vai poder ultrapassar que é o de violar essa autoridade entre aspas "interpretativa". Digo autoridade entre aspas porque na verdade essa autoridade tem que ser devidamente fundamentada, a ANPD não tem carta em branco para interpretar a LGPD como bem entender.

É interessante a ressalva feita pelo então Diretor de que a ANPD não teria uma "carta em branco" interpretativa da LGPD, porque remete ao posicionamento anterior da Secretaria – evidenciado na Nota Técnica nº 04/19 (citada anteriormente) – de parcimônia quanto à competência preponderante da Autoridade em casos envolvendo dados pessoais.

Desde então, outros acontecimentos na relação Senacon-ANPD deram indícios sobre a construção da relação institucional entre os dois órgãos. Em janeiro de 2021, o Conselho Nacional de Defesa do Consumidor (CNDC)[9] criou um núcleo especializado em proteção de dados. De

[8] A fala foi proferida em evento *on-line* sobre o uso de dados pessoais no cenário dos direitos do consumidor, organizado pela Associação Data Privacy Brasil. Os trechos citados são transcrições da fala do então Diretor do DPDC, Leonardo Albuquerque Marques, disponível em: https://www.youtube.com/watch?v=0P3aB8DCwL4. Acesso em: 21 fev. 2021.

[9] O Conselho Nacional de Defesa do Consumidor foi recriado em 2020 com a edição do Decreto 10.417/2020, com o intuito de ser o "espaço institucional e democrático para o desenho de políticas públicas nacionais de defesa do consumidor, baseadas nas melhores práticas internacionais, no qual

acordo com a então Secretária Nacional do Consumidor, Juliana Domingues, o objetivo de criar um núcleo especializado seria de "aproximação institucional" com a ANPD, para "promover o diálogo e mais segurança jurídica, uma vez que há vários temas interdisciplinares que envolvem a proteção de dados dos consumidores brasileiros"[10].

O segundo acontecimento se deu em fevereiro de 2021, quando a Senacon e a ANPD firmaram um Acordo de Cooperação Técnica, que, de acordo com o que foi veiculado no portal de notícias do endereço eletrônico da ANPD, teria por intuito a "uniformização de entendimentos e uma atuação coordenada no endereçamento de reclamações de consumidores", em que "a ANPD, por sua vez, fixará as interpretações necessárias à aplicação da Lei Geral de Proteção de Dados (LGPD)" nas "dezenas de casos sendo investigados pelo Departamento de Proteção e Defesa do Consumidor (DPDC) da Senacon".

Nesse sentido, desde a materialização da Autoridade Nacional de Proteção de Dados, Senacon e ANPD aparentam uma relação de cooperação institucional. Em especial, é interessante notar que essa cooperação parece se desenvolver na direção de uma atuação conjunta e articulada desses dois órgãos. Em entrevista realizada no âmbito desta pesquisa com um ex-servidor da Senacon, foi relatada a impressão de que haveria "uma atuação bastante harmônica [com a ANPD] porque acaba que, por estarem no governo, as agências têm uma limitação orçamentária grande e elas precisam muito umas das outras".

Além disso, vale ressaltar que, no âmbito da fiscalização do cumprimento da LGPD, há na lei a previsão expressa da competência de organismos de defesa do consumidor para o recebimento de petições individuais em relação aos direitos de proteção de dados[11]. E, de fato, a Senacon continuou instaurando procedimentos administrativos sobre o tema, mesmo após a institucionalização da ANPD.

representantes federais, estaduais e municipais de órgãos de defesa do consumidor terão assento", conforme escreveu o então Secretário Nacional do Consumidor, Luciano Benetti Tim (2020).

[10] A nota de imprensa publicada pela Senacon está disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/secretaria-nacional-do-consumidor-se-reune-com-anpd-para-tratar-de-acordo-para-protecao-de-dados-dos-consumidores. Acesso em: 24 nov. 2021.

[11] A possibilidade de peticionamento perante os organismos de defesa do consumidor está prevista no art. 18, § 8º, da LGPD: "o direito a que se refere o § 1º deste artigo [de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional] também poderá ser exercido perante os organismos de defesa do consumidor".

Nesse sentido, vale citar a recomendação conjunta[12] elaborada pela Senacon, pelo Ministério Público Federal, pelo Cade e pela ANPD sobre a atualização da política de privacidade do WhatsApp, que, de acordo com os órgãos, poderia representar violações aos direitos dos titulares de dados pessoais. Além desse caso de cooperação interinstitucional, ocorreram outros de maior protagonismo da Secretaria. Por exemplo, as sanções aplicadas contra diversas instituições financeiras entre maio e julho de 2021 em decorrência do uso indevido de dados de idosos sem o seu consentimento[13].

Por fim, em agosto de 2021, a Senacon lançou a campanha "Proteja seus dados. Não compartilhe"[14] no mês de aniversário de um ano da entrada em vigência da LGPD. E, em setembro do mesmo ano, lançou, em conjunto com a ANPD, um guia de conscientização do consumidor sobre "Como proteger seus dados pessoais", em evento da Secretaria que comemorava os 31 anos do Código de Defesa do Consumidor (CDC)[15].

Vale esclarecer que o objeto desta pesquisa não é analisar a relação entre a ANPD e a Senacon, ou questões relacionadas à preponderância da competência da ANPD em relação a outros órgãos públicos. Esta introdução teve por objetivo apresentar o contexto institucional e normativo em que o objeto desta pesquisa se insere. E, sobretudo, demonstrar a atualidade e a relevância de se atentar para a atuação da Senacon enquanto parte do arranjo institucional brasileiro de proteção de dados pessoais.

Desde 2018, percebe-se que a Senacon tem atuado no campo da proteção de dados. Nesse contexto, é relevante analisar como o regime jurídico da tutela dos dados pessoais vem sendo aplicado pela Secretaria, em especial, como o Direito tem sido mobilizado – "em ação" – nas decisões dos procedimentos administrativos envolvendo dados pessoais em trâmite na Senacon.

Para tanto, este trabalho se divide em seis partes. A primeira parte elabora sobre os objetivos da pesquisa. A segunda, aborda a relação da pesquisa com o campo do direito e desenvolvimento.

---

[12] A recomendação conjunta do MPF, Senacon, CADE e ANPD no caso da atualização da Política de Privacidade do WhatsApp está disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/recomendacao_whatsapp_-_assinada.pdf. Acesso em: 24 nov. 2021.

[13] Esses casos foram apresentados no tópico 4.2.4.

[14] A nota de imprensa de divulgação do lançamento da campanha está disponível em: https://www.defesadoconsumidor.gov.br/portal/ultimas-noticias/1901-ministerio-da-justica-e-seguranca-publica-lanca-campanha-educativa-para-informar-consumidor-sobre-protecao-de-dados. Acesso em: 24 nov. 2021.

[15] A publicação *on-line* do Guia está disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/arquivos-de-documentos-de-publicacoes/guia-do-consumidor_como-proteger-seus-dados-pessoais-final.pdf. Acesso em: 24 nov. 2021.

A terceira, explica os materiais e dados analisados, bem como a metodologia adotada para a sua coleta e análise. A quarta, apresenta uma visão geral dos casos estudados, por meio da descrição qualitativa destes. A quinta, constrói a "gramática"[16] da proteção de dados adotada pela Secretaria a partir da identificação das "palavras-chave", isto é, as categorias conceituais que traduzem a forma do órgão de interpretar os casos estudados, com o intuito de compreender como a abordagem da Senacon à proteção de dados pessoais se relaciona com os conceitos, regras e pressupostos normativos advindos da LGPD.

Por fim, a pesquisa apresenta a sua conclusão no sentido de que, embora exista sobreposição e utilização de conceitos análogos aos da LGPD pela Senacon, a principal diferença entre a abordagem da Secretaria e o paradigma normativo da LGPD, que se fundamenta na ideia de prover mecanismos individuais de controle aos titulares de dados pessoais para garantir que eles possam exercer a sua autodeterminação informativa, se dá de forma mais proeminente na adoção pela Senacon do pressuposto normativo da vulnerabilidade do consumidor como lente interpretativa nas decisões sobre os "usos indevidos de dados". O reconhecimento da vulnerabilidade do consumidor como elemento central de análise fez com que a atuação da Secretaria fosse orientada à sua proteção, prescindindo de um enfrentamento de questões técnico-normativas que poderiam ser suscitadas caso as condutas fossem interpretadas pela ótica da LGPD. Essa abordagem protetiva ao consumidor diante de sua vulnerabilidade em decorrência do uso de seus dados pessoais é o que caracteriza a "gramática" adotada pela Secretaria nos casos estudados.

[16] A ideia de "gramática" adotada na pesquisa se inspirou no texto "The 'Rule of Law,' Political Choices and Development Common Sense" (KENNEDY, 2006), em que o autor utilizou a ideia de "*grammar*" para denotar a forma com que profissionais do campo do desenvolvimento mobilizavam diferentes *expertises* no desenho de políticas desenvolvimentistas. Em períodos sucessivos, profissionais do campo do desenvolvimento definiram "desenvolvimento" de forma distinta e apresentaram caminhos de desenvolvimento em termos distintos. O autor adota a ideia de "gramática" para delinear essas formas distintas de definir e propor os caminhos para o desenvolvimento, por vezes adotando perspectivas econômicas, políticas e do Direito.

1. OBJETIVOS DA PESQUISA

A pesquisa tem por objetivo compreender como a Senacon mobilizou o Direito nas 33 notas técnicas públicas conclusivas de averiguações preliminares e processos administrativos envolvendo dados pessoais que tramitaram na Secretaria entre fevereiro de 2019 e julho de 2021. Em especial, identificar as "palavras-chave", isto é, os conceitos que traduzem a "gramática" adotada pelo órgão para interpretar e decidir casos relacionados à tutela de dados pessoais, com o intuito de compreender como a abordagem da Senacon à proteção de dados pessoais se relaciona com os conceitos, as regras e os pressupostos normativos advindos da LGPD (Lei 13.709/2018).

O interesse de pesquisar a atuação da Senacon surgiu da curiosidade sobre o sentido da expressão "uso indevido de dados" adotada pelo órgão para classificar uma série de eventos distintos envolvendo dados pessoais nos casos investigados pelo DPDC, que integra a Secretaria[17]. Primeiro, porque não há na LGPD qualquer referência literal à expressão "uso indevido de dados". Segundo, porque, salvo raras exceções[18], o legislador não estabeleceu *a priori*, no texto legal, as hipóteses ou finalidades para as quais o uso de dados pessoais estaria vedado.

O dispositivo que define o que seria considerado um tratamento de dados pessoais irregular (art. 44 da LGPD) – possivelmente uma expressão análoga a "uso indevido de dados" – teve a sua configuração bastante aberta na legislação, adotando termos indeterminados, como: "deixar de observar a legislação", "não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes" e não considerar "resultado e riscos que dele razoavelmente se esperam", entre outras hipóteses, conforme se verifica na transcrição do dispositivo a seguir:

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

[17] Essas investigações estão sendo amplamente divulgadas pela mídia. Ver: https://valor.globo.com/brasil/noticia/2020/09/24/uso-de-empresas-de-fechada-para-venda-ilegal-de-dados-entra-na-mira-do-governo.ghtml; https://noticias.r7.com/economia/ofertas-nem-sempre-sao-fidedignas-alerta-senacon-sobre-black-friday-27112020; e https://tecnoblog.net/405877/senacon-e-procon-sp-notificam-serasa-sobre-vazamento-de-220-milhoes-de-cpfs/. Acesso em: 17 fev. 2021.

[18] Algumas dessas exceções são: (i) o uso compartilhado de dados de saúde com o objetivo de obter vantagem econômica (art. 11, § 4º, da LGPD); (ii) o tratamento de dados de saúde por operadoras de planos privados de assistência à saúde para a prática de "seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários" (art. 11, § 5º, da LGPD); e (iii) o tratamento por pessoa jurídica de direito privado para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigações e repressões de infrações penais (art. 4º, § 2º, da LGPD).

> I – o modo pelo qual é realizado;
> II – o resultado e os riscos que razoavelmente dele se esperam;
> III – as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
> Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Dada a competência de órgãos de defesa do consumidor receberem reclamações dos titulares de dados pessoais em relação aos direitos previstos na LGPD (art. 18, § 8º, da LGPD), a Senacon integra o arranjo institucional de proteção de dados pessoais no Brasil. Nesse contexto, é relevante compreender como a Secretaria tem aplicado o Direito nos casos de "uso indevido de dados".

A partir de uma análise exploratória das notas técnicas de conclusão dos procedimentos administrativos (averiguações preliminares e processos administrativos) que ocorreram entre fevereiro de 2019 e julho de 2021, foi possível identificar seis categorias de condutas classificadas pela Secretaria como "uso indevido de dados", sendo elas: (i) comercialização de dados pessoais; (ii) mecanismos de monitoramento ou vigilância; (iii) compartilhamento de dados pessoais com terceiros, sem a ciência ou autorização de seus titulares; (iv) uso dos dados para finalidades que seriam prejudiciais aos titulares dos dados; (v) vazamento de dados pessoais; e (vi) falhas de segurança da informação.

A partir dessa primeira experiência exploratória com as notas técnicas, um elemento que chamou a atenção foi a abordagem adotada pela Secretaria, em especial a forma da Senacon de traduzir os elementos objetivos dos casos por meio de conceitos jurídicos. Embora adotasse conceitos análogos ao previstos na LGPD, a Secretaria parecia partir de pressupostos normativos distintos desta. Essa percepção se desdobrou nas perguntas da presente pesquisa, sendo possível elaborá-las da seguinte forma: Quais conceitos traduzem a abordagem da Senacon aos procedimentos administrativos analisados no escopo da pesquisa? Como esses conceitos adotados pela Secretaria se relacionam com o paradigma conceitual-normativo da LGPD?

Por fim, vale adiantar que, por adotar como paradigma metodológico a *grounded-theory* (ou teorização fundamentada em dados), a pesquisa renuncia ao objetivo de se empenhar na verificação de uma ou mais hipóteses preestabelecidas a partir de dado referencial teórico, visando, por sua vez, a geração de hipóteses por meio do processo indutivo de análise dos dados, objetivando a criação de uma proposta teórica – enraizada a partir da observação da realidade empírica – que,

por seu turno, passa a ser objeto de avaliação, discussão e comparação, à luz de outras formulações teóricas já existentes (CAPPI, 2017, p. 397).

2. RELAÇÃO DA PESQUISA COM O DIREITO E DESENVOLVIMENTO

Há mais de quatro décadas, a Organização para a Cooperação e Desenvolvimento Econômico formava o seu primeiro grupo de especialistas com o intuito de criar diretrizes para a proteção da privacidade e a eliminação de barreiras para o fluxo internacional de dados. Essas diretrizes foram adotadas em 1980 pela Organização e ficaram conhecidas como "*OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*" (as "Diretrizes"), constituindo o primeiro *framework* de princípios de proteção à privacidade em âmbito global.

De acordo com Michael Kirby, juiz australiano que liderou o grupo de especialistas da OCDE para a formulação das Diretrizes, estas surgiram como uma resposta da Organização às iniciativas europeias de regulação sobre o tema que surgiam à época. O receio da OCDE girava em torno da possibilidade de as nações europeias construírem barreiras jurídicas e econômicas que atrapalhariam o livre fluxo internacional de dados, havendo suspeitas de que a estratégia europeia seria muito burocrática, altamente custosa de se implementar, insensível aos valores gerados pelos fluxos internacionais de dados e até possivelmente motivada por um protecionismo econômico europeu (KIRBY, 2011).

Apesar de as Diretrizes não serem vinculantes, a OCDE incentivou que todos os países-membros da Organização adotassem os seus princípios e cooperassem com outros países-membros na sua implementação, para que divergências regulatórias não surgissem na operacionalização das Diretrizes entre as diferentes nações. Ainda que não fossem vinculantes, as Diretrizes da OCDE influenciaram o desenho de legislações e tratados de proteção de dados pessoais ao redor do mundo, como a Convenção 108 do Conselho da Europa ("Convenção 108"), de 28 de janeiro de 1981, que foi ratificada por 40 Estados europeus, incluindo a Suíça (TENE, 2013). A Convenção 108 refletia tanto os conceitos quanto os princípios da Diretrizes da OCDE.

Contudo, o risco de os princípios da Convenção 108 serem implementados de forma desigual pelos Estados nacionais fez com que a Comissão Europeia elaborasse a Diretiva 95/46/EC (HUSTINX, 2011), que tinha por intuito garantir que os Estados-membros adotassem um esquema

regulatório compatível em relação ao tratamento de dados pessoais. Entretanto, a despeito desse objetivo, os Estados acabaram implementando 27 modelos distintos e, por vezes, conflitantes de proteção de dados (TENE, 2013).

Após três décadas, as primeiras legislações e tratados relacionados à proteção de dados pessoais passaram por um período de reforma, cujo produto Omar Tene (2013) denominou de normas globais de segunda geração de proteção da privacidade. Essas reformas buscavam modernizar os arranjos institucionais e regulatórios de proteção de dados para endereçar o rápido desenvolvimento das tecnologias da informação e da comunicação que ocorreriam à época. O notório aumento da capacidade de processamento de dados levou governos, empresas e indivíduos a perceberem um maior valor sobre o uso e tratamento de dados.

No território europeu, o projeto de reforma da Diretiva Europeia teve início em 2010, mesmo ano em que o Ministério da Justiça brasileiro abria a sua primeira consulta pública sobre o Anteprojeto de Lei de Proteção de Dados Pessoais. Em comunicação direcionada ao Parlamento Europeu intitulada "*A comprehensive approach on personal data protection in the European Union*" (2010), a Comissão Europeia sustentava que "o rápido desenvolvimento tecnológico e a globalização mudaram profundamente o mundo ao nosso redor e trouxeram novos desafios para a proteção de dados pessoais" e que "as formas de coleta de dados pessoais têm se tornado cada vez mais elaboradas e menos facilmente detectáveis", convocando a União Europeia a desenvolver "uma abordagem abrangente e coerente, que garanta o direito fundamental à proteção de dados para os indivíduos de forma integral, dentro da UE e fora dela".

O processo de reforma do arranjo europeu de proteção de dados teve como resultado o Regulamento Geral de Proteção de Dados Europeu (UE) 2016/679 (*General Data Protection Regulation* – GDPR). Por ser um regulamento, o GDPR mudou a sistemática de coordenação e aplicação normativa de proteção de dados na Europa, já que os termos do Regulamento – diferente da Diretiva – eram diretamente aplicáveis a todos os países-membros, prescindindo de necessidade da incorporação às jurisdições nacionais (DONEDA, 2019, p. 199).

Conforme já mencionado anteriormente, o processo legislativo da LGPD foi influenciado pelas iniciativas e processos de reforma das legislações citadas anteriormente. Em depoimento ao Projeto Memória da LGPD, Danilo Doneda mencionou que, quando o Ministério da Justiça propôs

o Anteprojeto de Lei para discussão em 2010[19], já se percebia um processo internacional de uniformização de regras de proteção de dados: "Isso nem há dez anos, há vinte anos. Desde que a União Europeia tomou um passo decisivo nesse sentido" [20]. E vale ressaltar que um dos argumentos utilizados para pressionar a aprovação da LGPD no Congresso Nacional foi de que, para o Brasil entrar na OCDE, haveria a necessidade de seguir suas recomendações, por exemplo, adotando um sistema de proteção de dados pessoais compatível com as Diretrizes (SIMÃO; MORIBE, 2021).

Nesse sentido, pode-se dizer que a relação da pesquisa com o direito e desenvolvimento reside em seu objeto. De acordo com Mariana Mota Prado (2010), o direito e desenvolvimento é um campo que, atualmente, tem comportado uma série de estudos, abordagens, análises e temas. Ainda que, originalmente, tenha surgido com enfoque na relação entre o Direito e o desenvolvimento econômico (*law in development*), o seu enfoque se ampliou ao longo do tempo, passando a analisar o funcionamento de instituições e de liberdades e garantias individuais como desenvolvimento (*law as development*).

A presente pesquisa tem o segundo enfoque de *law as development*, se relacionando com o direito e desenvolvimento na medida em que busca analisar como tem se dado o enraizamento da proteção de dados pessoais no ordenamento jurídico brasileiro, considerando o seu contexto particular e as capacidades do arranjo regulatório preexistente para o seu desenvolvimento. Apesar de a proteção de dados pessoais brasileira aparentar "nos livros" uma grande influência dos debates internacionais de regulação da proteção de dados, em especial o europeu, faz sentido analisar de forma empírica e descrever, conceitualmente, como o direito à proteção de dados pessoais tem sido aplicado localmente – isto é, "em ação" – nas organizações que compõem o arranjo institucional de proteção de dados pessoais brasileiro.

---

[19] Trata-se de depoimento coletado a partir do projeto "Memória da LGPD", organizado pela Organização Data Privacy Brasil e citado anteriormente na nota 3. Disponível em: https://observatorioprivacidade.com.br/memorias/. Acesso em: 20 fev. 2021.

[19] Nos termos da exposição de vetos, "os dispositivos incorrem em inconstitucionalidade do processo legislativo, por afronta ao artigo 61, § 1º, II, 'e', cumulado com o artigo 37, XIX da Constituição". A exposição dos vetos está disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Msg/VEP/VEP-451.htm. Acesso em: 23 fev. 2021.

[20] Trata-se de depoimento coletado a partir do projeto "Memória da LGPD", organizado pela Organização Data Privacy Brasil e citado anteriormente na nota 3. Disponível em: https://observatorioprivacidade.com.br/memorias/. Acesso em: 20 fev. 2021.

[20] Nos termos da exposição de vetos, "os dispositivos incorrem em inconstitucionalidade do processo legislativo, por afronta ao artigo 61, § 1º, II, 'e', cumulado com o artigo 37, XIX da Constituição". A exposição dos vetos está disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Msg/VEP/VEP-451.htm. Acesso em: 23 fev. 2021.

3. METODOLOGIA

Esta seção tem o objetivo de explicar a metodologia adotada pela pesquisa. Em síntese, trata-se de uma pesquisa qualitativa, predominantemente documental, que utiliza a teorização fundamentada em dados (*grounded-theory*) para compreender os conceitos que traduzem a "gramática" adotada pela Secretaria Nacional do Consumidor nas investigações que conduziu sobre usos indevidos de dados pessoais. A análise foi feita a partir de dois tipos de material: notas técnicas e entrevista.

A seguir, há uma descrição sobre a forma que os materiais foram coletados, uma explicação sobre a metodologia adotada para análise dos dados, um detalhamento sobre a ferramenta usada para a codificação dos documentos e entrevista, bem como uma justificativa de adequação de cada uma dessas escolhas tendo em vista os propósitos e objetivos pretendidos pelo trabalho.

3.1. Os materiais

Para compreender como a Secretaria Nacional do Consumidor tem mobilizado o Direito e, em especial, os conceitos adotados por ela para decidir os procedimentos administrativos envolvendo dados pessoais, optou-se, inicialmente, pela estratégia de pesquisar a partir da combinação de dois tipos de materiais: notas técnicas de resolução das averiguações preliminares e processos administrativos e entrevistas com os servidores da Senacon envolvidos nos procedimentos administrativos estudados.

Contudo, conforme será mais bem elaborado no item 3.1.2 a seguir, a dificuldade de conseguir que os servidores participassem de entrevista para a pesquisa fez com que ela se tornasse predominantemente documental, isto é, fundada, prioritariamente, na análise qualitativa das notas técnicas. O conteúdo da única entrevista realizada foi utilizado para preencher de sentido as lacunas e demais questões implícitas inferidas da leitura e análise das notas técnicas, como o papel das empresas de auditoria e consultoria independentes na instrução probatória dos procedimentos administrativos.

A seguir, há uma explicação sobre a forma de coleta desses dois materiais, os desafios enfrentados para obtê-los, suas potencialidades e limitações.

3.1.1. Notas técnicas

A forma escolhida para analisar o modo como a Senacon tem mobilizado o Direito nos procedimentos que conduziu relacionados a dados pessoais foi a análise dos documentos das averiguações preliminares e processos administrativos que tramitaram na Secretaria envolvendo dados pessoais. Em um primeiro momento, houve a tentativa de acessar esses documentos via consulta no Sistema Eletrônico de Informações (SEI) do Governo Federal. Contudo, após uma série de tentativas utilizando palavras e expressões-chave, como "dados pessoais", "privacidade", "banco de dados" e "LGPD" (e suas variações), o mecanismo de consulta apenas retornou documentos institucionais da Senacon sobre o tema, como as notas técnicas elaboradas pelo órgão durante o processo legislativo da LGPD, não disponibilizando qualquer informação sobre as investigações relacionadas ao uso de dados pessoais de consumidores.

Dessa forma, em setembro de 2020, foi apresentado pedido de acesso à informação direcionado à Senacon via plataforma Fala.BR do governo federal[21] solicitando "acesso à íntegra de todos os documentos, tais como ofícios, processos administrativos e notas técnicas relacionados à proteção de dados pessoais ou à Lei nº 13.709/18, que ocorreram entre 14 de agosto de 2018 até a presente data". Vale dizer que o marco inicial de 14 de agosto de 2018 foi escolhido por se tratar da data de sanção da LGPD.

Em 7 de outubro de 2020, a Coordenação-Geral de Sanções Administrativas da Secretaria indeferiu o pedido de acesso à informação apresentado em razão da "amplitude e generalidade do pedido", recomendando que fossem mais bem detalhados "o escopo e a abrangência da solicitação" feita ao DPDC, alegando, ainda, que documentos relacionados aos procedimentos estariam protegidos por sigilo, "por se tratar de informações comerciais relevantes ou estratégias de mercado" das organizações investigadas.

Em paralelo, as investigações sobre "uso indevido de dados" eram amplamente divulgadas na mídia[22]. Com isso, em 9 de outubro de 2020, foi apresentado recurso de 1ª instância contra a resposta apresentada pela Secretaria, sustentando que a generalidade da solicitação se justificava na medida em que essas informações não estavam disponíveis para consulta via SEI, não existindo,

[21] Disponível em: https://www.gov.br/acessoainformacao/pt-br. Acesso em: 2 nov. 2021.
[22] *Vide* nota 17.

portanto, a possibilidade de apresentar de forma específica a numeração dos autos ou a totalidade de investigações, processos e termos envolvendo dados pessoais. E, com o intuito de trazer maior especificidade à solicitação, foi anexada ao recurso entrevista concedida pela então Secretária Nacional do Consumidor, Juliana Domingues, ao jornal *Valor Econômico*, na qual ela afirmava que 34 processos administrativos relacionados ao uso indevido de dados pessoais tramitavam naquele momento perante a Secretaria[23]. Com relação à alegação sobre sigilo, o recurso foi no sentido de reiterar que o art. 7º da Lei de Acesso à Informação assegura o acesso às demais informações (não sigilosas), ocultando-se a parte sigilosa (por meio da utilização de tarjas pretas para supressão das partes sigilosas, por exemplo).

Em outubro, o então Diretor do Departamento de Proteção e Defesa do Consumidor, Leonardo Marques, deferiu parcialmente o recurso, informando que disponibilizaria o "acesso às Notas Técnicas Públicas, de condenação e/ou de instauração, excluindo-se os que se encontram em Averiguação Preliminar e os documentos constantes dos processos que contenham dados sigilosos das Representadas".

Com o intuito de obter um acesso mais amplo aos documentos das investigações, foi apresentado recurso de 2ª instância ao Ministro de Estado da Justiça e Segurança Pública solicitando que fosse, adicionalmente, conferido acesso aos seguintes documentos:

> 1) Cópia das notificações instauradoras de investigação preliminar (conforme art. 42, Decreto nº 2.181/97) movidas pelo Departamento de Proteção e Defesa do Consumidor (DPDC) em temas relacionados à proteção de dados pessoais, que ocorreram de 1º de agosto de 2018 até a presente data; 2) Cópia das notificações instauradoras de processo administrativo (conforme art. 39, Decreto nº 2.181/97) movidos pelo Departamento de Proteção e Defesa do Consumidor (DPDC) em temas relacionados à proteção de dados pessoais, que ocorreram de 1º de agosto de 2018 até a presente data; 3) Cópia dos Termos de Ajustamento de Condutas já firmados pela Senacon em temas relacionados à proteção de dados pessoais de 1º de agosto de 2018 até a presente data; e 4) Cópia das decisões dos Processos Administrativos e Averiguações Preliminares do Departamento de Defesa de Proteção ao Consumidor (DPDC) relacionadas à proteção de dados pessoais de 1º de agosto de 2018 até a presente data.

Em novembro, o Ministro de Estado da Justiça e Segurança Pública deferiu o recurso de 2ª instância, mas não versou sobre o pedido de acesso a outros documentos, limitando-se a determinar um prazo de 90 dias para a concessão das informações não sigilosas. Em fevereiro de 2021, a Coordenação de Transparência e Acesso à Informação do Ministério disponibilizou 26 notas

[23] Disponível em: https://valor.globo.com/brasil/noticia/2020/09/24/uso-de-empresas-de-fechada-para-venda-ilegal-de-dados-entra-na-mira-do-governo.ghtml. Acesso em: 2 nov. 2021.

técnicas que versavam sobre as conclusões do DPDC em averiguações preliminares e processos administrativos sobre proteção de dados, no período de julho de 2019 a agosto de 2020.

Tendo em vista o êxito na obtenção desses documentos via Lei de Acesso à Informação, para acessar o maior número possível de notas técnicas para a pesquisa, foram realizados outros quatro pedidos de acesso à informação, com o intuito de obter as notas técnicas emitidas pela Senacon no período de sanção da LGPD até o seu primeiro ano de vigência (14.08.2018 a 18.09.2021). No total, foram fornecidas 33 notas técnicas, tendo a primeira sido emitida pela Secretaria em 6 de fevereiro de 2019 e a última, em 14 de julho de 2021. No "Apêndice A" deste trabalho consta uma relação das notas técnicas analisadas no escopo da pesquisa.

Vale dizer que, para a Senacon, a nota técnica é:

> (...) um documento elaborado por técnicos especializados em determinado assunto e difere do Parecer pela análise completa de todo o contexto, devendo conter histórico e fundamento legal, baseados em informações relevantes. É emitida quando identificada a necessidade de fundamentação formal ou informação específica da área responsável pela matéria e oferece alternativas para tomada de decisão.[24]

E, no presente contexto, a nota técnica foi o instrumento adotado pela Secretaria para formalizar as decisões tomadas por ela nos procedimentos administrativos de fiscalização e sanção que conduziu. Vale ressaltar que as 33 notas técnicas obtidas via Lei de Acesso à Informação podem não compreender todo o universo de procedimentos administrativos que tramitaram na Secretaria. Ainda que o pedido tenha sido para a obtenção de todas as notas técnicas, as 33 notas técnicas analisadas estão limitadas às notas técnicas públicas disponibilizadas pelo órgão a seu exclusivo critério, não sendo possível avaliar a completude em relação às decisões que ocorreram no período.

De qualquer forma, os documentos disponibilizados incluem casos de grande repercussão nacional, como o uso de tecnologia de reconhecimento facial pela Hering em uma de suas lojas, a transcrição de áudios da ferramenta Messenger pelo Facebook e o "escândalo" do caso *Cambridge Analytica*. Portanto, mesmo que possivelmente o material não contemple a totalidade das decisões tomadas no período pela Secretaria, entendeu-se que ele seria adequado aos objetivos deste trabalho, pelos seguintes motivos: (i) envolvem casos diversos e interessantes; (ii) não estão disponíveis publicamente; e (iii) a nota técnica é um documento completo para análise da forma de

[24] Conforme definição disponível em: https://www.defesadoconsumidor.gov.br/portal/biblioteca/95-notas-tecnicas. Acesso em: 24 nov. 2021.

interpretar e decidir da Senacon, uma vez que apresenta as circunstâncias fáticas, os argumentos de defesa das empresas investigadas, bem como a fundamentação da Secretaria ao decidi-los.

3.1.2. Entrevistas

Inicialmente, o intuito da pesquisa era complementar a análise documental das notas técnicas disponibilizadas pela Secretaria com o conteúdo de entrevistas semiestruturadas realizadas com servidores da Senacon. Isso porque as entrevistas teriam a potencialidade de acrescentar uma nova camada à análise, qual seja, dos elementos políticos, institucionais e organizacionais presentes na atuação da Secretaria durante as investigações, mas que não estivessem evidentes nas notas técnicas, seja pela falta de interesse ou custo político de divulgação, seja pela incompatibilidade do conteúdo com o instrumento da nota técnica. Por exemplo, questões como limitações de capacidade institucional do órgão, atritos e interesses político-institucionais, bem como mudanças interpretativas decorrentes das trocas de gestão e pessoal da Secretaria.

Nesse sentido, a seleção de potenciais entrevistados foi feita a partir da identificação dos servidores envolvidos na condução dos casos a partir dos nomes e cargos que constavam na assinatura das notas técnicas. No total, onze servidores distintos assinaram uma ou mais das notas técnicas estudadas. Com os nomes em mãos, um processo de busca ativa dos endereços eletrônicos de contato foi iniciado, por meio do diretório de busca do Google, assim como outras plataformas disponíveis publicamente – por exemplo, Lattes – CNPQ e Linkedin – e endereços de contatos disponibilizados na identificação de artigos acadêmicos.

Encontrados os endereços eletrônicos, foram enviados os convites para a participação na pesquisa, bem como o Termo de Consentimento Livre e Esclarecido, conforme aprovado pelo Comitê de Conformidade Ética em Pesquisas Envolvendo Seres Humanos da FGV. Sobre isso, vale ressaltar que alguns cuidados adicionais tiveram de ser tomados, considerando a atuação profissional da pesquisadora no campo estudado. Esses cuidados incluíram o compromisso de limitar a finalidade de uso das informações coletadas ao âmbito da pesquisa conduzida e a transparência com o entrevistado sobre a atuação profissional da pesquisadora. Além disso, possibilitou-se a todos os potenciais entrevistados a possibilidade de participação anônima na pesquisa.

Das onze comunicações inicialmente enviadas, foram obtidas quatro respostas de servidores e ex-servidores interessados em participar da entrevista ou saber mais sobre a pesquisa[25]. Para aqueles que não responderam, foram feitas mais de uma tentativa de contato. Das quatro respostas obtidas, apenas dois deles aceitaram participar da pesquisa, de forma anônima. Um dos servidores que tinha aceitado participar da entrevista teve de remarcar a conversa por duas vezes e, ao fim, indicou outro servidor para conceder a entrevista em seu lugar, mas este não se sentiu confortável em participar da pesquisa, com receio de se "comprometer funcionalmente".

Nesse sentido, ao final, apenas uma entrevista pôde ser realizada, que ocorreu em agosto de 2021. A entrevista se deu de forma remota e contou com um roteiro semiestruturado de perguntas, que incluíam questões como "*como você avalia o impacto das decisões da Senacon em proteção de dados nos últimos anos?*", "*existe uma mudança de entendimento sobre proteção de dados na Senacon conforme as mudanças de gestão?*", "*na sua percepção, qual o papel da Senacon em temas envolvendo dados pessoais antes da criação da ANPD? Na sua percepção, o que muda a partir da constituição da ANPD? Quais as razões para o protagonismo ou não?*", entre outras questões gerais sobre a percepção do ex-servidor sobre a atuação da Senacon nos casos envolvendo a tutela de dados pessoais. Além dessas perguntas gerais, previamente à entrevista, foram elaboradas questões específicas relacionadas aos casos em que o ex-servidor em questão esteve envolvido.

A despeito de ter ocorrido apenas uma entrevista com um ex-servidor, ela foi determinante para o acesso a uma dimensão interna da Secretaria, pela perspectiva de um profissional que fez parte do seu quadro e que evidenciou questões sobre como capacidades institucionais do órgão se relacionam com as decisões da Senacon. Por exemplo, em diversos casos a Secretaria realiza reuniões presenciais com os representados e as atas dessas reuniões não constam no texto das notas técnicas. Contudo, não é raro que, após a reunião, as representadas apresentem relatórios de auditoria realizados por empresas especializadas ou consultoria independentes. Na entrevista, foi possível saber que uma das maiores limitações institucionais do órgão se relaciona com a capacidade técnica para a produção e análise de prova dos eventos investigados, especialmente quando os casos envolvem temas que exigem um alto nível de *expertise* em sistemas da informação,

[25] Para garantir a anonimidade dos convidados e participantes, as informações serão utilizadas na pesquisa de forma não identificada, mencionando apenas a denominação genérica de "servidor", conforme preferência do participante.

como ocorre nos casos de incidentes de segurança da informação (ex.: vazamento de dados). E, conforme relatado pelo entrevistado, por esse motivo, era comum que, durante as reuniões realizadas com as empresas investigadas, a Secretaria propusesse aos representados a apresentação de relatório técnico produzido por uma dessas empresas de auditoria, com análise técnica de impacto e gravidade dos eventos investigados, notadamente em casos envolvendo incidentes de segurança da informação.

Concluindo, ante a dificuldade de realizar mais entrevistas, a pesquisa acabou adotando um enfoque predominantemente documental, em que o conteúdo da única entrevista realizada foi utilizado de forma complementar à análise documental para preencher as possíveis lacunas de sentido. Disso decorre uma das principais limitações do trabalho, que é não conseguir capturar com precisão possíveis mudanças interpretativas durante a troca de gestão e questões político-institucionais que afetam a atuação da Secretaria e como isso se relaciona com a "gramática" adotada por ela. A despeito dessa limitação, para o objetivo do presente trabalho, a fundamentação jurídica adotada pela Secretaria nas notas técnicas foi suficiente para permitir a identificação dos conceitos adotados por ela.

3.2. A metodologia: Teorização Fundamentada em Dados (*grounded-theory*)

Tendo em vista o objetivo da pesquisa de identificar os conceitos jurídicos que traduzem a "gramática" adotada pela Secretaria Nacional do Consumidor nas investigações sobre proteção de dados, a *grounded-theory* – ou teorização fundamentada em dados (TFD) – foi a metodologia escolhida. Conforme Ricardo Cappi (2017), a TFD viabiliza ao pesquisador "compreender – e formular teoricamente – o ponto de vista e as significações construídas pelos atores sociais num 'campo' específico" (p. 401), dedicando-se "especificamente à compreensão das maneiras pelas quais os sujeitos observados raciocinam e interpretam a realidade" (p. 402), incluindo as "maneiras de pensar, as maneiras de definir as situações e de conceber as ações" (p. 402), permitindo uma análise profunda sobre "as práticas, os discursos e/ou as ideias – e as relações entre estes elementos – dos atores sociais e jurídicos, em determinado contexto e determinada situação" (p. 403).

A *grounded-theory* – ou teorização fundamentada em dados (TFD) – é uma metodologia que surgiu em 1967, com a publicação da obra *The Discovery of Grounded Theory*, de autoria dos sociólogos Barney G. Glaser e Anselm L. Strauss. Essa obra surge no campo das ciências sociais

em um momento em que métodos quantitativos tinham maior predominância e métodos qualitativos eram considerados imprecisos e pouco rigorosos. A TFD aparece com o intuito de endereçar as críticas feitas então à pesquisa qualitativa, introduzindo uma metodologia que permitiria a teorização por meio da coleta e análise sistemática de dados (STRAUSS; CORBIN, 2008).

Desde a sua concepção, a *grounded-theory* evoluiu em caminhos distintos do original positivismo de Glauser e Strauss (BRYANT; CHARMAZ, 2019). Esta pesquisa adota a proposta de Kathy Charmaz (2006) para a TFD, que incorpora as diretrizes originais da *grounded-theory*, mas assume como referencial epistemológico o construtivismo e como perspectiva teórica o interacionismo simbólico (CROTTY, 1998). Assim, a TFD de Charmaz incorpora a subjetividade do observador no processo metodológico, conforme se verifica no trecho transcrito a seguir:

> Grounded theory serves as a way to learn about the worlds we study and a method for developing theories to understand them. In the classic grounded theory works, Glaser and Strauss talk about discovering theory as emerging from data separate from the scientific observer. Unlike their position, I assume that neither data nor theories are discovered. Rather, we are part of the world we study and the data we collect. We construct our grounded theories through our past and present involvements and interactions with people, perspectives, and research practices.

As reflexões de Charmaz apontadas anteriormente são pertinentes para esta pesquisa. Isso porque a autora do presente trabalho atua profissionalmente no campo estudado. Nesse sentido, a curiosidade que deu origem ao objeto de estudo decorreu, em parte, da relação e formação profissional da pesquisadora com o campo. Portanto, é importante ressaltar ao leitor que, além da vivência acadêmica, a vivência profissional da pesquisadora no campo interagiu de alguma forma para o desenvolvimento da pergunta de pesquisa, bem como do processo de análise dos dados[26].

[26] A pergunta de pesquisa sobre como o arranjo de proteção de dados pessoais se enraíza no ordenamento jurídico brasileiro surge a partir de uma vivência profissional no campo. Com a entrada em vigor do GDPR na Europa em maio de 2018, empresas brasileiras multinacionais com sede no Brasil começaram a procurar apoio jurídico para a adequação de suas atividades e serviços à nova norma europeia nos escritórios de advocacia locais. A autora deste trabalho iniciou o exercício da advocacia nesse contexto, em um dos primeiros escritórios de advocacia brasileiros a contar com uma área especializada sobre o tema. Além disso, em agosto de 2018, a LGPD é sancionada com um período de *vacatio legis* de dois anos para que as organizações impactadas pudessem se adaptar às novas regras. Contudo, a sanção não é acompanhada da constituição – naquele momento – de uma autoridade regulamentadora para orientar "como" deveria ser a adequação das operações de tratamento de dados pessoais pelas organizações da iniciativa pública e privada. Ainda, a LGPD, por ser uma norma geral, com caráter principiológico, de aplicação setorialmente transversal, foi editada com uma linguagem por vezes bastante aberta, surgindo com várias lacunas e possibilidades interpretativas. Diante desse contexto, de uma perspectiva profissional, houve a necessidade de buscar em diretrizes estrangeiras os parâmetros para a interpretação da LGPD, em especial no GDPR (por exemplo, o sentido de dado pessoal e dado anonimizado, a possibilidade de

Inobstante, o papel acadêmico pôde ser desenvolvido de forma independente, tendo a pesquisadora se colocado o ônus de garantir que a interação entre ambos os papéis não comprometesse o efetivo exercício da liberdade acadêmica durante o desenvolvimento da pesquisa. Isso foi feito a partir de um exercício de conscientização sobre possíveis vieses interpretativos, com o intuito de perceber e controlar eventuais projeções oriundas do papel de advogada sobre a análise dos dados.

Feita essa breve introdução, explica-se, então, o processo metodológico do uso da *grounded-theory* na pesquisa. A TFD, originalmente formulada por Glauser e Strauss, adotava algumas premissas, as quais Charmaz adota como um conjunto de princípios e práticas de pesquisa, passível de flexibilização conforme as necessidades de cada trabalho. As premissas da TFD adotadas pelo presente trabalho foram: (i) códigos analíticos e categorias devem ser construídos a partir dos dados e não de hipóteses dedutivas anteriores; (ii) memorandos devem ser elaborados durante o processo de análise dos dados para o desenvolvimento das categorias conceituais, especificando suas propriedades, definindo a relação entre elas e identificando eventuais lacunas de significado; (iii) a amostragem dos dados é voltada à teorização ("*theoretical sampling*"), isto é, seu objetivo é melhor capturar as propriedades e dimensões das categorias conceituais, e não apresentar uma representatividade estatística dessas categorias; e (iv) a revisão bibliográfica ocorre após o processo de análise dos dados para garantia do processo indutivo de interpretação (CHARMAZ, 2006).

O processo metodológico aconteceu em camadas. Inicialmente, foi feita a coleta das notas técnicas, conforme narrado no tópico anterior. Posteriormente, iniciou-se o processo de leitura e codificação desses documentos utilizando o software Atlas.ti[27]. A primeira etapa de codificação foi

aplicação do legítimo interesse, a classificação de controladores e operadores de dados em casos limítrofes, entre outros). Paralelamente, outras autoridades locais começaram a atuar em casos envolvendo o uso de dados pessoais, como a Senacon. Dessa experiência surgiu também o lampejo de compreender como os casos relacionados a dados pessoais estavam sendo interpretados pelas autoridades locais, quais conceitos jurídicos estavam sendo utilizados e os sentidos em que esses conceitos eram aplicados, consideradas a trajetória e capacidades institucionais desses órgãos.

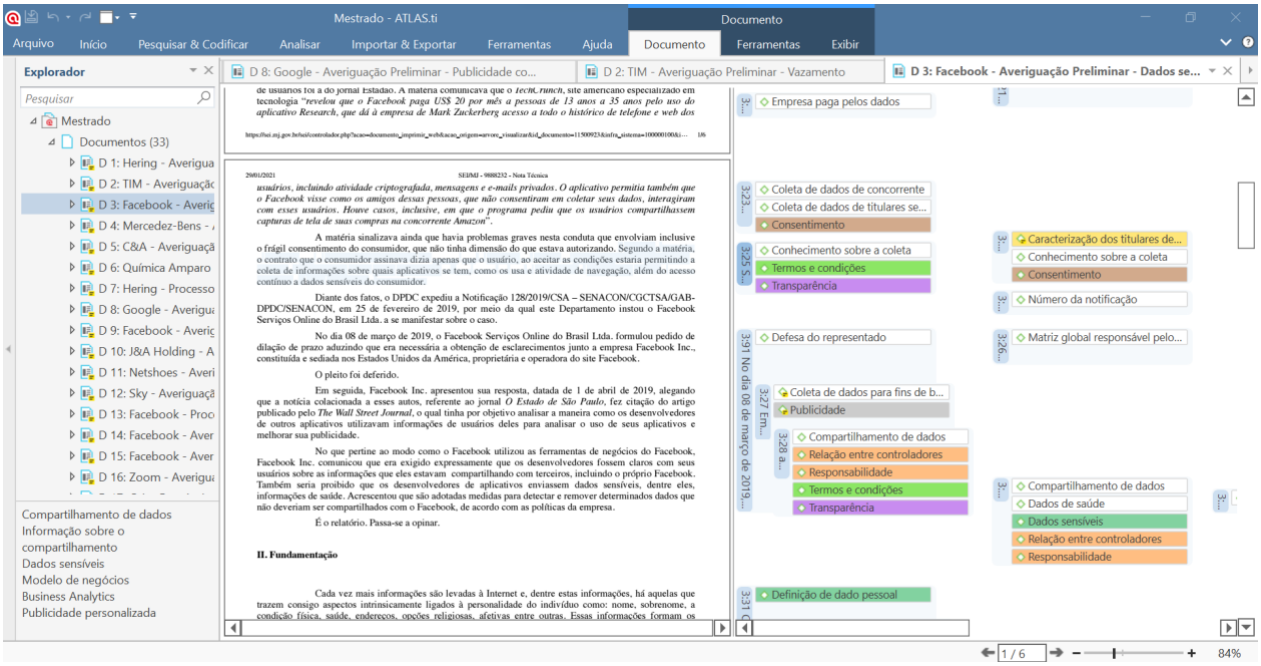
[27] O *software* Atlas.ti é um programa de computador que foi desenvolvido para facilitar a análise qualitativa de dados. A licença do *software* é paga e temporária. Mais informações sobre o programa podem ser encontradas no endereço eletrônico da empresa desenvolvedora: https://atlasti.com/. Vale ressaltar que todo o processo de análise foi feito de forma manual, não tendo a pesquisa utilizado as ferramentas de automatização de análise disponíveis no programa. A opção por fazê-lo de forma manual se dá pela opção de utilizar o software como uma ferramenta para a codificação e análise, e não como um substituto da pesquisadora. Por fim, sobre o uso de *software* para apoiar o processo de análise, cabe transcrever aqui uma reflexão de Corbin sobre o tema (2008): "*In every seminar that I've taught over the past years, there is the inevitable question about the use of computer programs for qualitative analysis. Though the use of computer programs in qualitative research is debatable and outright rejected by some researchers,*

feita em um baixo nível de abstração entre texto e código, usando como unidade de registro[28] períodos frasais, conforme a figura ilustrativa a seguir. Ao todo, foram codificados 2.446 excertos ("citações", na nomenclatura do *software*).

computer programs for analysis are here to stay and their ability to support the research process increases with each improvement in the many programs that are available. Notice that I say 'support' and not 'take over' or 'direct' the research process. I think one of the most interesting aspects of this edition is that it demonstrates that the analytic process remains a researcher-driven thinking and feeling process, even with the supplementation of a computer program. This is a very important point. Though users of computer programs sometimes rigidify the analytic process, this need not be. The evolving analysis should determine how the researcher will use the computer program and not the reverse. There is no reason to restrict analysis to the limits of a program's capabilities. Computer programs are tools, like the many other analytic tools presented in this book. They can enhance the ability of the researcher to search for, store, sort, and retrieve materials. They help a researcher keep track of his or her codes, provide easy access to memos, and facilitate the making of diagrams. Furthermore, the researcher need not be committed to an analytic scheme too early in the analytic process because computer programs allow the researcher to move materials around and think about them in other ways. Everything is at the analyst's fingertips. There is no more rummaging through boxes or notebooks looking for that important memo. Finally, computer programs provide for transparency of the research process. The researcher can retrace the analytical process, an option that didn't exist twenty years ago".

[28] Conforme Charmaz (2006, p. 47-66), a codificação pode adotar uma série de estratégias, as quais variam de acordo com a unidade de registro escolhida para a elaboração dos códigos. Na TFD, a unidade de registro poderia ser palavra por palavra, linha por linha, incidente por incidente, *in vivo*, direcionada, axial ou teórica. Essa pesquisa mesclou as estratégias de codificação, adotando como regra o registro de códigos por período frasal, mas com codificação complementar por incidente e *in vivo*. Isso significa que um código foi atribuído a cada período frasal. Essa menor granularidade, de acordo com os teóricos da *grounded-theory*, é uma forma de garantir o enraizamento da teoria aos dados, uma vez que há um esforço de atribuir sentido a cada linha, mitigando o risco de projeção ou enviesamento na análise dos dados. A codificação por incidente foi adotada especialmente para questões mais estruturais do documento, por exemplo, atribuindo um código a mais de um parágrafo quando se tratava, por exemplo, dos argumentos de defesa da representada ou então a forma que a Senacon calculava a dosimetria das sanções. A codificação *in vivo*, isto é, que utiliza os mesmos termos da Secretaria como códigos, foi adotada em casos em que havia o uso reiterado de determinada expressão, por exemplo, uso indevido de dados ou prática abusiva.

Imagem 1 – Processo de codificação utilizando o software Atlas.ti[29]



Fonte: imagem da autora.

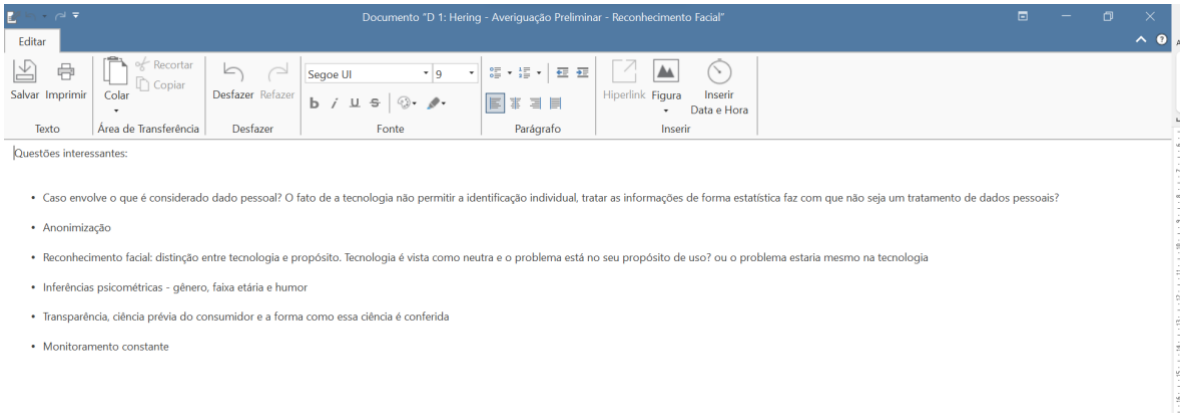
Durante o processo de codificação em baixo nível de abstração foram identificados 467 códigos, que são as marcações coloridas no canto direito da figura 1, *supra*.

Ao final da leitura e codificação de cada nota técnica (unidade de "documentos", no Atlas.ti), observações, pontos de atenção, conceitos interessantes, tais como a forma como ideias eram articuladas, como os eventos investigados eram descritos e qualificados, entre outras questões pertinentes à análise, eram descritos em memorandos[30], conforme exemplo ilustrativo a seguir:

[29] Mais informações sobre a ferramenta disponíveis em: https://www.youtube.com/watch?v=43C0d0uu_yU. Acesso em: 6 mar. 2022.

[30] Memorandos foram escritos tanto no nível de análise das notas técnicas para designar pontos de atenção e de interesse em cada documento, quanto no nível dos códigos, para indicar observações ou percepções de sentido de possíveis categorias conceituais e suas relações durante o processo de codificação.

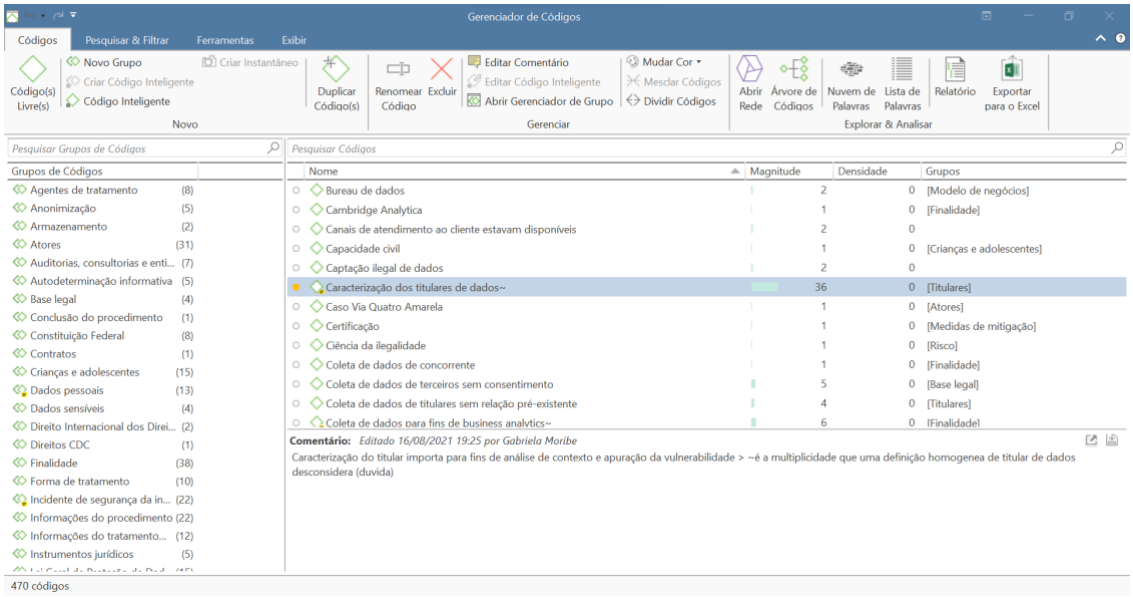
Imagem 2 – Processo de elaboração de memorandos usando a ferramenta de “comentários” no nível do documento utilizando o software Atlas.ti



Fonte: imagem da autora.

A segunda etapa do processo de codificação foi partir dos códigos com um médio nível de abstração para categorias conceituais (as “palavras-chave”), agrupando os códigos a partir de seu conteúdo semântico (por exemplo, “empresas independentes de auditoria”) e/ou de sua afinidade com um conceito jurídico já existente no Direito (como “consentimento”, “responsabilidade” e “prática abusiva”), conforme se verifica na figura 3 a seguir. Ao todo, foram identificados 46 grupos de códigos.

Imagem 3 – Ferramenta “gerenciador de códigos” do Atlas.ti, utilizada para agrupamento de códigos em categorias conceituais

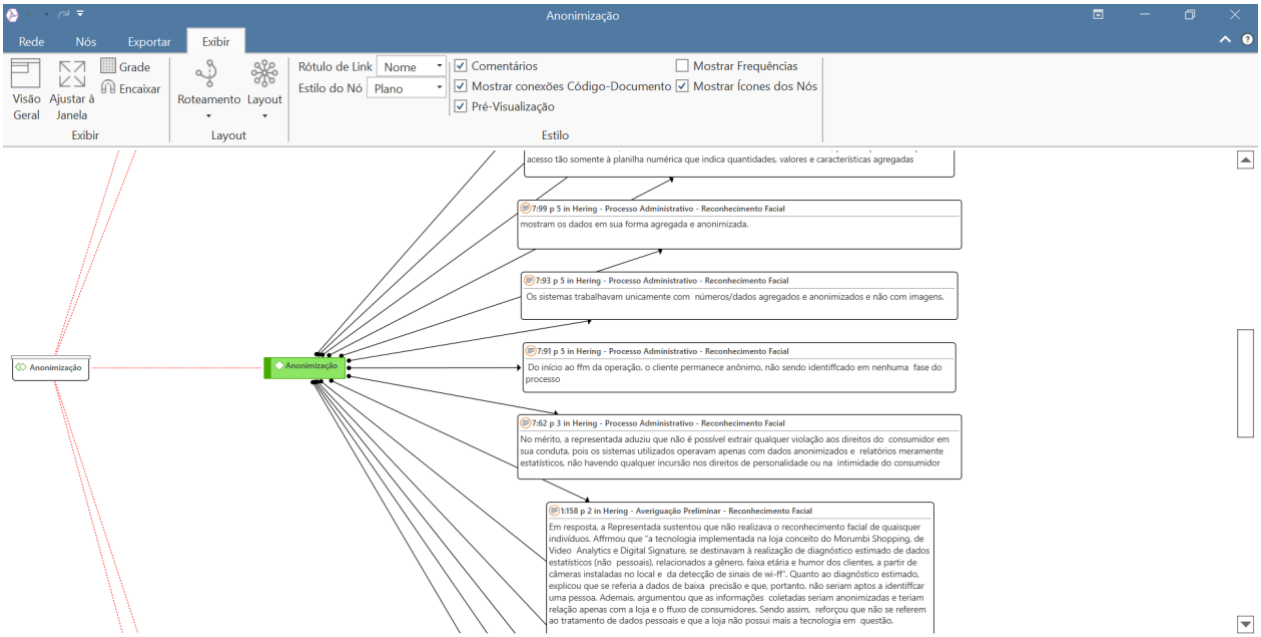


Fonte: imagem da autora.

Em paralelo com o processo de codificação das notas técnicas, foi realizada a entrevista com um ex-servidor da Senacon, cujo conteúdo também foi codificado. Entretanto, a codificação da entrevista, por se tratar de um dado complementar à análise documental, foi feita de forma direcionada ao preenchimento de sentido das categorias conceituais identificadas a partir da codificação das notas técnicas.

O conjunto dessas categorias conceituais (palavras-chave) compõe o que a pesquisa denomina de "gramática". Identificadas as categorias conceituais, a pesquisa analisa qualitativamente cada uma delas, articulando a forma como tais conceitos são empregados pela Secretaria, com as possíveis definições para esses mesmos conceitos, nos termos da LGPD. Para essa etapa de análise, a ferramenta de "rede" do Atlas.ti foi utilizada para visualizar a relação entre as citações (excertos codificados), os códigos a elas relacionados, bem como seu agrupamento em uma categoria conceitual, conforme ilustração exemplificativa, a seguir, do conceito de anonimização:

Imagem 4 – Ferramenta "rede" do Atlas.ti, utilizada para identificar as relações entre excertos do texto (citações) codificados sob a mesma categoria conceitual (grupo de códigos)[31]



Fonte: imagem da autora.

[31] Mais informações sobre a ferramenta disponíveis em: https://www.youtube.com/watch?v=P6AlJxTaXvI. Acesso em: 6 mar. 2022.

Vale ressaltar que ao todo foram identificadas 46 categorias conceituais, dentre as quais foram selecionadas as oito palavras-chave mais relevantes para o desenvolvimento teórico na quinta parte deste trabalho. Com o intuito de garantir a síntese dos conceitos, em alguns casos, fez sentido mesclar alguns grupos de código em uma mesma categoria conceitual. Isso aconteceu com os conceitos de "consentimento" e "base legal", já que consentimento está contido em base legal; "dado pessoal" e "dado pessoal sensível", visto que dado sensível é parte da categoria de dado pessoal; e "uso indevido de dados" e "prática abusiva". Conforme pertinente e para maior clareza para o leitor, as nuances das propriedades e dimensões das categorias conceituais e seus elementos foram delineados em maior profundidade nas palavras-chave da quinta parte.

Com isso, a pesquisa buscou identificar os oito principais conceitos que traduzem a "gramática" adotada pela Senacon, analisando a relação da abordagem da Senacon à proteção de dados pessoais com os conceitos, regras e pressupostos normativos advindos da LGPD (Lei 13.709/2018). Essa lista de conceitos será apresentada na pesquisa em ordem alfabética, tendo inspiração na obra *Keywords: a vocabulary of culture and society*, de Raymond Williams (1983), que será retomada no tópico 5 deste trabalho.

4. OS CASOS DE PROTEÇÃO DE DADOS PESSOAIS NA SECRETARIA NACIONAL DO CONSUMIDOR

Este tópico apresenta uma visão geral dos casos estudados na pesquisa em quatro partes. A primeira parte tem o intuito de descrever a forma como a Secretaria Nacional do Consumidor legitima a sua competência para atuar nesses casos por meio do DPDC. A segunda tem como objetivo apresentar um panorama geral sobre as investigações, descrevendo as condutas investigadas pela Secretaria. A terceira aborda os demais atores que apareceram nas notas técnicas, sendo eles organizações da sociedade civil, autoridades públicas nacionais e internacionais e entidades do setor privado com quem a Senacon dialoga e/ou interage nos procedimentos administrativos. Por fim, a quarta seção tem o objetivo de apresentar quais são os principais dispositivos jurídicos mobilizados pela Secretaria enquanto regras do Direito que teriam sido violadas pelas empresas investigadas.

4.1. A Senacon e o DPDC

A Secretaria Nacional do Consumidor foi criada pelo Decreto 7.738/2012, como um órgão integrante do Ministério da Justiça[32] com competência para "receber, analisar, avaliar e encaminhar consultas, denúncias ou sugestões apresentadas por entidades representativas ou pessoas jurídicas de direito público ou privado" (art. 106, II, do CDC e art. 3º, II, do Decreto 2.181/1997), bem como "fiscalizar e aplicar as sanções administrativas previstas na Lei nº 8.078, de 11 de setembro de 1990 , e em outras normas pertinentes à defesa do consumidor" (art. 3º, X, do Decreto 2.181/1997 e art. 17, VIII, do Decreto 9.662/2019).

Nas 33 notas técnicas públicas analisadas, o argumento de legitimidade e competência para a atuação da Secretaria é construído a partir da ideia de que no Sistema Nacional de Defesa do Consumidor (SNDC) os órgãos e entidades que o integram têm competência concorrente no exercício do poder de polícia administrativa, cabendo à Senacon o papel de coordenação da política do SNDC.

E, no âmbito da coordenação do SNDC, a Secretaria é assessorada pelo DPDC, cujas competências estão previstas no art. 18 do Decreto 9.662/2019 e no Regimento Interno da Senacon (Portaria 905/2017, do Ministério da Justiça e Segurança Pública). Dentre essas competências, nas notas técnicas, há, reiteradamente, menção expressa às seguintes atribuições:

> a) assessorar a Senacon na formulação, na promoção, na supervisão e na coordenação da política nacional de proteção e defesa do consumidor, bem como na articulação e na coordenação do sistema nacional de defesa do consumidor; b) solicitar à polícia judiciária a instauração de inquérito para a apuração de delito contra os consumidores e representar ao Ministério Público, para fins de adoção das medidas necessárias ao cumprimento da legislação de defesa do consumidor, no âmbito de sua competência; c) comunicar e propor aos órgãos competentes medidas de prevenção e repressão às práticas contrárias aos direitos dos consumidores e fiscalizar demandas que envolvam relevante interesse geral e de âmbito nacional, além de aplicar as sanções administrativas previstas nas normas de defesa do consumidor e instaurar averiguações preliminares e processos administrativos[33].

É pelo DPDC que a Secretaria instaura os procedimentos administrativos estudados nesta pesquisa. Além do DPDC, a Senacon conta também com o Sistema Nacional de Informações de Defesa do Consumidor (Sindec), que é o sistema informatizado de registro das demandas individuais dos consumidores que recorrem aos Procons, consolidando bases locais para a

[32] Posteriormente transformado em Ministério da Justiça e Segurança Pública durante o governo Bolsonaro (2019 – presente; sem partido).
[33] Por exemplo, na nota técnica nº 19/2020/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ.

formação de um banco nacional de informações sobre problemas enfrentados pelos consumidores[34]. O Sindec foi utilizado pela Senacon para a atuação baseada em evidências nas investigações das instituições financeiras que serão explicadas a seguir.

Além disso, vale dizer que, por compor a Administração Pública Federal, a Secretaria está suscetível a mudanças decorrentes de troca de gestão. Durante a entrevista com um antigo servidor da Secretaria, questionou-se se as mudanças de gestão afetavam a forma como os casos eram decididos, oportunidade em que o entrevistado afirmou o seguinte:

> O perfil da gestão dita muito um padrão, (...) não um padrão de processo, as regras continuam iguais, os procedimentos continuam iguais, isso não é influenciado. Lá dentro mesmo existe uma liberdade muito grande dos servidores tomarem decisões, ou de não tomarem decisões também. Não existe esse tipo de pressão de "vamos decidir assim por causa dessa gestão", isso não acontecia. O que acontecia era: uma nova gestão entrava e, por exemplo, uma pessoa que tem um maior apreço pelo tema de tecnologia foca no tema de tecnologia. Isso, sim, pode acontecer. E isso era uma coisa que acontecia, a gente percebia lá dentro que, (...) um exemplo aleatório: o tema de publicidade infantil foi um tema muito forte numa gestão, se não me engano, de 2016-2017. A gente soltou algumas decisões sobre isso. Na última gestão que eu trabalhei, não era um tema que existia assim uma punição tão forte, uma repressão tão forte, a gestão enxergava de uma outra forma. Então isso impacta de fato, quais processos são abertos, quais têm um andamento mais célere, isso existe sim.

4.2. Os casos investigados

O Decreto nº 2.181/97 organiza o SNDC e disciplina as normas gerais de aplicação das sanções administrativas previstas no CDC. Na pesquisa, foram analisados dois tipos de procedimentos administrativos, que são regulados pelo Decreto: averiguações preliminares e processos administrativos.

De acordo com o Decreto, a averiguação preliminar é um mecanismo opcional colocado à disposição dos órgãos do SNDC, que antecede o processo administrativo e tem por intuito requisitar das organizações reclamadas maiores informações sobre as questões e práticas investigadas (art. 33, § 1º, Decreto nº 2.181/97). O resultado de uma averiguação preliminar pode ser tanto o seu arquivamento, quanto a abertura de processo administrativo sancionador, a depender da avaliação do órgão sobre as informações levantadas. Já o processo administrativo é a instância de instrução e julgamento das atividades fiscalizatórias das relações de consumo pelos órgãos de

[34] Informações extraídas do *site* do Sindec, que podem ser acessadas em: https://sindecnacional.mj.gov.br/sobre. Acesso em: 5 dez. 2021.

defesa do consumidor (art. 4º, IV, Decreto nº 2.181/97), podendo ter como resultado o seu arquivamento ou a aplicação de sanções administrativas (art. 18 e seguintes, Decreto nº 2.181/97).

Das 33 notas técnicas analisadas, 26 eram decisões de averiguações preliminares e 7, de processos administrativos. A partir de uma análise do teor das notas técnicas, foram identificadas quais seriam as condutas caracterizadas como "*uso indevido de dados*" de acordo com a Senacon. São elas: (i) comercialização de dados pessoais; (ii) mecanismos de monitoramento ou vigilância; (iii) compartilhamento de dados pessoais com terceiros, sem a ciência ou autorização de seus titulares; (iv) uso dos dados para finalidades que seriam prejudiciais aos titulares dos dados; (v) vazamento de dados pessoais; e (vi) falhas de segurança da informação, categorias que são explicadas a seguir.

4.2.1. Comercialização de dados pessoais

A primeira categoria está relacionada a organizações investigadas pela Secretaria pela suposta prática de comercializar dados pessoais de consumidores. Essas organizações foram: C&A Modas S.A. (C&A) e J&A Holding Ltda. (J&A Holding).

No caso da C&A[35], a Senacon instaurou uma averiguação preliminar em razão de notícia veiculada na mídia com imagens e vídeos que aparentemente mostravam funcionários das lojas C&A vendendo dados de consumidores cadastrados na empresa para "criminosos na internet". De acordo com a nota técnica, fotos de cartões de crédito, documentos pessoais e assinaturas coletados pela empresa estariam sendo comercializados "pelo valor mínimo de R$ 50,00 (cinquenta reais) por pessoa, e fichas cadastrais de consumidores por um preço que variava entre R$ 50 e R$ 150".

O DPDC descreveu a conduta como "exposição de dados dos consumidores". Apurados os fatos durante a averiguação preliminar, a decisão da Secretaria foi pelo arquivamento do caso em razão da "atuação proativa da Representada, por meio da contratação de consultoria independente para a identificação de possíveis vulnerabilidades de segurança existentes em seus sistemas e ferramentas, bem como a elaboração de plano de ação destinado à correção desta" (2020, p. 6). Além disso, "o comprometimento dos dados também" não teria sido "amplamente verificado" (2020, p. 6).

[35] Nota Técnica nº 19/2020/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.002376/2017-88.

O segundo caso, da J&A Holding[36], foi instaurado de ofício pelo DPDC após veiculação na mídia de que "empresas privadas comercializavam dados pessoais, inclusive financeiros, de brasileiros", citando nominalmente a *holding*. Na nota técnica, há reprodução de trecho da matéria, transcrito a seguir:

> (...) além das informações das centenas de milhares de clientes serem facilmente obtidas, eles vendem essas informações privadas por uma nova empresa do grupo (Assert Tecnologia + Stormtech) (...) Além dos dados de pessoas físicas, eles possuem informações de todas as empresas do Brasil. De alguma forma eles possuem os dados de INSS de toda a população e eles vendem essa informação através dos sites (http://consulta .plus/ e http://app.asserttecnologia.com.br/) (...) Os dados de INSS estão expostos nessa URL para quem quiser baixar (...) Através de uma rápida análise nos e-mails internos da empresa, constata-se que eles tem total ciência que não poderiam vender esses dados, inclusive fazendo a empresa de advocacia deles trabalhar numa garantia jurídica, envolvendo mentiras como contratos fakes entre empresas do grupo e de que essas informações são obtidas da navegação dos usuários nos sites e parceria com as outras empresas do grupo.

O caso foi descrito pelo DPDC como "comercialização de dados pessoais e sigilosos de consumidores". A conclusão do Departamento foi curiosamente pela sugestão de arquivamento do procedimento, em razão de o DPDC não ter conseguido localizar a empresa e ter identificado que o endereço cadastrado por ela junto à Receita Federal seria desconhecido dos Correios, o que o órgão entendeu como um indício de que a empresa teria sido constituída de forma fraudulenta e que provavelmente já teria sido extinta.

4.2.2. Mecanismos de monitoramento ou vigilância

A segunda categoria relaciona quatro casos que teriam como elemento comum práticas de monitoramento ou vigilância de consumidores. As organizações investigadas em razão dessas condutas foram: Facebook Inc. (Facebook), Google Brasil Internet Ltda. (Google) e Cia Hering (Hering).

O Facebook esteve envolvido em dois casos dessa categoria. No primeiro[37], a empresa teria contratado serviço terceirizado para escutar e transcrever gravações de voz (áudios) de usuários de seus serviços, tais como o Messenger. De acordo com a nota técnica, teria sido noticiado pela mídia

[36] Nota Técnica nº 378/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo n° 08012.001400/2019-23.
[37] Nota Técnica nº 10/2020/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.002596/2019-73.

que “os funcionários das empresas contratadas ouvem as conversas dos usuários do Facebook, mas não sabem por que o Facebook as quer transcritas”. Segundo a matéria, o intuito dessa prática seria o aprimoramento da ferramenta de inteligência artificial do Facebook e a revisão de conteúdos que possivelmente violassem as políticas da rede social.

O DPDC descreveu essa conduta como “transcrição de áudios de usuários sem autorização”. A conclusão do Departamento sobre o caso foi de sugestão de arquivamento, uma vez que o recurso de “voz para texto” teria sido disponibilizado apenas aos usuários localizados nos Estados Unidos da América, inexistindo elementos probatórios de que usuários localizados em território brasileiro tivessem sido afetados pela prática.

O segundo caso do Facebook[38] foi uma averiguação preliminar instaurada em decorrência de uma notícia que denunciava a “utilização de dados sensíveis, como frequência cardíaca e ciclo menstrual, mensagens e e-mails privados, bem como localização do consumidor e visualização de bens imóveis” obtidos pelo Facebook a partir de integrações técnicas com outros aplicativos para a finalidade de “segmentar anúncios para consumidores na rede social”, isto é, para a publicidade comportamental, personalizada de acordo com o perfil de interesses inferido a partir do comportamento dos usuários.

Esta ocorrência foi descrita pelo Departamento como “compartilhamento indevido e sem consentimento de dados sensíveis de consumidores para fins publicitários”. Nesse caso, o DPDC sugeriu a instauração de processo administrativo, em razão dos indícios de que os consumidores não estariam “sendo devidamente informados sobre a coleta dos dados pessoais e quais dados estão sendo repassados”, especialmente os dados sensíveis. Não foi provido acesso à nota técnica do processo administrativo correlato.

O Google também esteve envolvido em dois casos nessa categoria. O primeiro[39] foi uma averiguação preliminar envolvendo a coleta de dados de geolocalização de crianças e adolescentes usuários do aplicativo YouTube (como localização, aparelho usado e número de telefone) com a finalidade de direcionar publicidade ao público infantil. O Departamento descreveu essa conduta como “coleta de dados de crianças, sem o devido consentimento, para fins publicitários”. A conclusão do DPDC para o caso foi de sugerir a instauração de procedimento administrativo.

[38] Nota Técnica nº 362/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.000520/2019-11.
[39] Nota Técnica nº 407/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.002781/2019-68.

O segundo procedimento[40] foi sobre o escaneamento do conteúdo de e-mails pessoais de usuários da plataforma Gmail para fins comerciais, investigado em averiguação preliminar iniciada por representação do Ministério Público Federal – Procuradoria da República no Estado do Piauí. Nesse procedimento, o DPDC decidiu pela instauração de processo administrativo sancionador, cuja nota técnica de desfecho não foi provida pela Secretaria[41].

Por fim, o caso da Hering envolveu duas notas técnicas, sendo uma da averiguação preliminar[42] e a outra do processo administrativo[43], ambas referentes à mesma conduta de monitoramento da reação dos clientes às roupas por meio de tecnologia de reconhecimento facial em uma das lojas da Companhia. A tecnologia denominada "VideoAnalytics" tinha dois objetivos: a produção de um "mapa de calor que demonstrava os pontos mais frequentados da loja" e a indicação de "gênero, faixa etária e humor dos consumidores no ambiente da loja", dados que eram obtidos "a partir de uma única câmera instalada próximo ao caixa". A averiguação preliminar levou ao processo administrativo e, em ambos os casos, a conduta da Hering foi descrita pelo DPDC como "utilização de tecnologia de reconhecimento facial para a coleta de dados de consumidores sem conhecimento prévio e consentimento". A conclusão do DPDC no processo administrativo foi pela aplicação de sanção administrativa no valor de R$ 58.767,00 à Hering.

4.2.3. Compartilhamento irregular de dados pessoais

A terceira categoria de conduta se caracteriza pelo compartilhamento de dados pessoais coletado dos consumidores com terceiros, sem que os titulares dessas informações tivessem ciência ou fornecido seu consentimento para a transferência de seus dados. As empresas que estiveram

[40] Nota Técnica nº 33/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.004630/2015-11.

[41] Em alguns casos, como neste, foram concedidas pela Secretaria as notas técnicas conclusivas de averiguações preliminares em que a Secretaria conclui pela instauração de processo administrativo. Contudo, nos pedidos de acesso à informação subsequentes, a Secretaria não disponibilizou acesso às notas técnicas dos processos administrativos em referência. Não é possível ter certeza do motivo de não concessão desses documentos. Contudo, é possível ventilar algumas hipóteses. Primeiro, que as notas técnicas dos processos administrativos sequer existem, em razão da prescrição intercorrente do procedimento administrativo, ou que a Secretaria, de forma deliberada ou acidental, não organizou internamente o documento do processo administrativo em conjunto com a nota técnica da averiguação preliminar e, por esse motivo, não concedeu acesso ao documento.

[42] Nota Técnica nº 294/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.001387/2019-11.

[43] Nota Técnica nº 62/2020/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.001387/2019-11.

envolvidas em investigações dessa categoria foram Facebook Inc. (Facebook) e Zoom Video Communications Inc. (Zoom).

O caso do Facebook envolve as notas técnicas da averiguação preliminar[44] e do processo administrativo[45] relacionadas ao escândalo do *Cambridge Analytica*. E começou a ser investigado pelo DPDC após notícia veiculada pela mídia, segundo a qual usuários brasileiros do Facebook poderiam

> (...) ter sofrido com o uso indevido de dados pela Cambridge Analytica. Ao todo, segundo a rede social, 87 milhões em todo o mundo podem ter tido suas informações compartilhadas pela consultoria de marketing político, sendo 70 milhões nos Estados Unidos. No Brasil, segundo nota publicada pelo Facebook em sua página na internet, este número foi de 443 mil.

O Departamento classificou a ocorrência como "exposição de consumidores brasileiros, decorrente da prestação do serviço com vício". A sugestão do DPDC foi de aplicação da sanção administrativa de multa, no valor de R$ 6.600.000,00 (seis milhões e seiscentos mil reais).

O segundo caso dessa categoria foi a averiguação preliminar da plataforma de videoconferências Zoom[46], que teve início em decorrência de notícia veiculada pela mídia, segundo a qual

> (...) a versão iOS do aplicativo Zoom está enviando alguns dados de análise para o Facebook, mesmo que os usuários do Zoom não tenham uma conta no Facebook, de acordo com uma análise do aplicativo na placa-mãe (...) O aplicativo Zoom notifica o Facebook quando o usuário abre o aplicativo, detalhes sobre o dispositivo do usuário, como o modelo, o fuso horário e a cidade da qual eles estão se conectando, de qual operadora de telefone eles estão usando e um identificador de anunciante exclusivo criado pelo dispositivo do usuário que as empresas podem usar para direcionar um usuário com anúncios.

A conduta foi descrita pelo DPDC como "exposição de dados de consumidores" e a decisão da Secretaria foi de sugerir o arquivamento do procedimento, dada "a disposição da representada em atender as solicitações deste Departamento e a disposição em oferecer ao consumidor brasileiro o mesmo standard de práticas de privacidade e de segurança da informação oferecidos ao usuário americano do aplicativo em estudo", práticas que teriam sido fruto de um compromisso da plataforma com a *Federal Trade Commission*, órgão de fiscalização americano.

---

[44] Nota Técnica nº 108/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.000723/2018-19.

[45] Nota Técnica nº 32/2019/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.000723/2018-19.

[46] Nota Técnica nº 67/2020/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.000760/2020-41.

4.2.4. Usos prejudiciais aos titulares dos dados pessoais

A quarta categoria de conduta se caracteriza pela utilização dos dados para uma finalidade concreta que é prejudicial aos titulares dessas informações. As empresas que estiveram envolvidas em investigações desta categoria eram Mercedes-Benz do Brasil Ltda. (Mercedez), Banco BMG S.A. (BMG), Banco Bradesco S.A. (Bradesco), Banco Bradesco Financiamentos S.A. (Bradesco Financiamentos), Banco Cetelem S.A. (Cetelem), Banco Pan S.A. (Pan), Banco do Estado do Rio Grande do Sul S.A. (Banrisul), Banco Itaú Consignado S.A. (Itaú Consignado), Banco Olé Bonsucesso Consignado S/A (Olé), Banco Safra S.A. (Safra) e Caixa Econômica Federal (Caixa).

O caso da Mercedes-Benz[47] foi uma averiguação preliminar baseada em notícia segundo a qual todos os carros produzidos na União Europeia eram obrigados a ter o sistema de transmissão de dados de geolocalização denominado "e-call", o qual deveria ser ativado apenas em situações emergenciais. Contudo, a afiliada da Mercedes do Reino Unido teria admitido publicamente que "rastreava os carros de seus clientes e que se servia dessas informações para localizar e recuperar veículos de clientes inadimplentes".

O caso foi descrito pelo DPDC como "utilização do e-call (sistema de transmissão de dados e geolocalização) na Europa, de forma indevida, com a finalidade de rastrear consumidores inadimplentes". E a conclusão do Departamento foi pela sugestão de arquivamento da Averiguação, pois não seria possível obter, a partir dos dados presentes no processo de homologação desses veículos perante o Denatran, se o fabricante estaria empregando o sistema de transmissão de dados e geolocalização "e-call" nos veículos comercializados em território brasileiro.

Os casos das instituições financeiras[48] tiveram notas técnicas muito semelhantes e todos decorreram de uma reclamação apresentada pelo Instituto de Defesa do Consumidor (Idec), que continha a seguinte denúncia:

---

[47] Nota Técnica nº 8/2020/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.002762/2019-31.

[48] Respectivamente, Nota Técnica nº 243/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.001478/2019-48; Nota Técnica nº 250/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.001489/2019-28; Nota Técnica nº 249/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.001488/2019-83; Nota Técnica nº 248/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.001476/2019-

> (...) instituições financeiras, mediante vazamento de dados dos aposentados e pensionistas vinculados ao Instituto Nacional do Seguro Social – INSS, estão realizando abordagens telefônicas de forma abusiva para que consumidores idosos adquiram empréstimo ou cartão de crédito consignado. Há registro, ainda, de que mesmo antes de auferir o primeiro benefício, os idosos estão a receber diversos contatos telefônicos com oferta de produtos na modalidade consignada. Segundo a denúncia apresentada, referida prática está levando os idosos a situação de superendividamento.

Em todos os casos o DPDC descreveu a existência de "indícios de prática de abusos na oferta e de violação de dados pessoais do idoso". Ainda, perante todas as instituições financeiras citadas, sugeriu que fossem instaurados processos administrativos.

A Secretaria forneceu as notas técnicas dos processos administrativos do Safra[49], Pan[50], Cetelem[51], BMG[52] e Itaú Consignado[53], sendo que a todas as cincos instituições financeiras aplicou sanção administrativa de multa, por identificar "conduta abusiva na oferta e concessão de empréstimos consignados" em decorrência de "abordagem nociva por telefone de idosos aposentados e pensionistas do INSS", "ausência de informação clara e adequada e violação de dados pessoais de idosos", configurando "exploração da hipervulnerabilidade do idoso". Respectivamente, as sanções foram de R$ 2,4 milhões; R$ 8,8 milhões; R$ 4 milhões; R$ 5,1 milhões; e R$ 9,6 milhões.

4.2.5. Vazamento de dados pessoais

59; Nota Técnica nº 247/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.001462/2019-35; Nota Técnica nº 246/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.001490/2019-52; Nota Técnica nº 245/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.001470/2019-81; Nota Técnica nº 244/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.001483/2019-51; Nota Técnica nº 242/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.001486/2019-94; e Nota Técnica nº 231/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.001492/2019-4.

[49] Nota Técnica nº 56/2021/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo Administrativo nº 08012.001486/2019-94.

[50] Nota Técnica nº 35/2021/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo Administrativo nº 08012.001462/2019-35.

[51] Nota Técnica nº 28/2021/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo Administrativo nº 08012.001476/2019-59.

[52] Nota Técnica nº48/2021/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo Administrativo nº 08012.001478/2019-48.

[53] Nota Técnica nº 40/2021/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo Administrativo nº 08012.001470/2019-81.

A quinta categoria de conduta está relacionada a vazamento dos dados pessoais dos consumidores. As organizações envolvidas com essa categoria foram: NS2.com Internet S.A. (Netshoes), Tim Celular S.A. (Tim), Química Amparo Ltda. (Química Amparo) e Facebook Inc. (Facebook).

O caso da Netshoes[54] foi uma averiguação preliminar instaurada em decorrência de notícia veiculada pelo Ministério Público do Distrito Federal e Territórios (MPDFT) informando que "cerca de 1.999.704 contas com informações de usuários cadastrados no site de compras da Representada teriam sido expostas". Em resposta, o MPDFT teria recomendado "que a Representada entrasse em contato com todos os seus clientes/consumidores afetados e que se abstivesse de efetuar qualquer tipo de pagamento ao suposto autor do incidente de segurança". A "notícia revelou também que o ocorrido comprometeu informações relativas ao nome, CPF, e-mail, data de nascimento e histórico de compras, mas não relativas a senhas ou cartão de crédito dos usuários do site Netshoes".

O DPDC descreveu esse evento como uma "exposição de dados pessoais dos consumidores" e sugeriu o arquivamento dessa averiguação preliminar ante

> (...) a celebração de Termo de Ajustamento de Conduta (TAC) entre o Ministério Público do Distrito Federal e Territórios e a Representada, em que além do pagamento de R$ 500.000,00 (quinhentos mil reais), relativo à indenização de danos morais coletivos, firmou-se a implementação de medidas adicionais ao Programa de Proteção de Dados, além de terem sido adotadas todas as providência à época para minimização dos efeitos das exposição dos dados dos clientes/consumidores.

O caso da Tim[55] envolveu averiguação preliminar instaurada após a Secretaria tomar conhecimento de uma notícia segundo a qual "existiria uma brecha, na plataforma Tim Negocia, que permitia que cibercriminosos acompanhassem dados pessoais e valores de dívidas de consumidor". O DPDC descreveu o evento como "vazamento de dados sensíveis e valores de dívidas dos consumidores" e sugeriu a instauração de processo administrativo, uma vez que a operadora de telefonia teria "exposto indevidamente os dados de seus clientes na plataforma Tim Negocia (então gerida por entidade terceirizada contratada pela Representada), permitindo que terceiros pudessem extrair dados ali guardados relativos aos seus consumidores sem que estes

[54] Nota Técnica nº 379/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo n. 08012.000145/2018-11.
[55] Nota Técnica nº 310/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.001392/2019-15.

últimos tivessem dado qualquer consentimento em tal sentido". Nesse caso, o DPDC decidiu pela abertura de processo administrativo sancionador, cuja nota técnica não foi disponibilizada pela Secretaria[56].

O caso da Química Amparo[57] foi um processo administrativo sobre uma falha de segurança da informação que expôs temporariamente dados de consumidores que participavam de campanha promocional da marca Ypê. De acordo com a notícia que denunciava a falha de segurança, os dados expostos por essa falha de segurança incluíam nome, CPF, data de nascimento, e-mail, telefone e senha. O DPDC descreveu a conduta como "vazamento de dados pessoais de consumidores" e decidiu por sugerir o arquivamento do procedimento, dada a "não gravidade do incidente, nos termos dos relatórios emitidos por empresas independentes" apresentados pela empresa durante o processo administrativo.

Por fim, o caso do Facebook[58] foi uma averiguação preliminar instaurada de ofício para "apuração de aparentes irregularidades cometidas por hackers que teriam invadido contas de usuários brasileiros cadastrados na plataforma Facebook e coletado dados pessoais, tais como: nome, e-mail, número de telefone, locais visitados e buscas realizadas pela internet", em setembro de 2018. O DPDC descreveu a conduta como "vazamento de informações pessoais". A conclusão do DPDC foi no sentido de sugerir a instauração de processo administrativo, cuja nota técnica não foi fornecida pela Secretaria.

4.2.6. Falhas de segurança da informação

A sexta e última categoria de conduta está relacionada a falhas técnicas de segurança da informação. Essa categoria se distingue da anterior porque, nestes casos, as falhas não acarretaram um vazamento de dados pessoais de consumidores, ao passo que a correção das falhas técnicas por parte dessas organizações teria sido suficiente para impedir o seu acesso por terceiros. As organizações envolvidas nessa categoria foram: Sky Serviços de Banda Larga Ltda. e Facebook Inc.

---

[56] *Vide* nota 42, *supra*.

[57] Nota Técnica nº 42/2020/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08000.030856/2019-30.

[58] Nota Técnica nº 109/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.002467/2018-02.

O caso da Sky[59] foi uma averiguação preliminar instaurada em decorrência de notícia veiculada na mídia sobre a exposição de dados, incluindo "nome completo, e-mail, senha de login do serviço, endereço de IP, métodos de pagamento, número de telefone e endereço residencial" de 32 milhões de consumidores brasileiros clientes da operadora de telefonia na internet. De acordo com a notícia, por meio do uso de recursos avançados de pesquisa, ter-se-ia identificado a possibilidade de acessar o banco de dados da Sky sem que houvesse mecanismos de autenticação ou proteção adicionais contra o acesso indevido.

O DPDC descreveu o caso como "exposição de dados de consumidores" e sugeriu o arquivamento do procedimento, em razão de a Sky ter adotado "as medidas reparatórias necessárias, tratando-se de medidas gerais de proteção e medidas técnicas de proteção, a fim de garantir a devida proteção do consumidor e de seus dados". Adicionalmente, a decisão citou ainda que investigação paralela instaurada pelo MPDFT teria concluído que a "Representada adotou as providências para o saneamento das falhas de segurança como a ausência de demonstração de vazamento de dados de seus clientes".

O segundo caso classificado dentro dessa categoria foi uma averiguação preliminar instaurada contra o Facebook[60] em razão de notícia veiculada na mídia alegando que "540 milhões de dados de usuários do Facebook ficaram expostos em servidores da Amazon, sem qualquer tipo de senha para acesso". De acordo com a notícia, "os dados, que eram requisitados por desenvolvedores de aplicativos para o Facebook, continham curtidas, comentários, fotos, músicas, informações sobre amigos, eventos e até reservas de voos e hotéis".

O caso foi classificado pelo DPDC como "exposição de dados de consumidores" e o Departamento concluiu pela sugestão de arquivamento do procedimento, uma vez que os desenvolvedores de aplicativos relacionados ao incidente não teriam usuários brasileiros como público-alvo, inexistindo indícios de que consumidores localizados no Brasil tivessem sido afetados significativamente pelo evento.

4.3. Os atores

[59] Nota Técnica nº 395/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.003074/2018-16.
[60] Nota Técnica nº 75/2020/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, Processo nº 08012.001086/2019-89.

Nas averiguações preliminares e nos processos administrativos, a Senacon interage com outros atores de diferentes maneiras. De acordo com o servidor da Secretaria entrevistado,

> (...) para ter um pouco mais de segurança das decisões da Senacon, existe uma interlocução muito grande com órgãos parceiros justamente por essa dificuldade de perícia, de provas. E aí entra uma parceria muito grande com outros órgãos, principalmente o Ministério Público. O MPDFT tem um núcleo muito forte de proteção de dados e aqui em Brasília eles ajudavam bastante a gente.

Este tópico busca apresentar as organizações com quem esse diálogo ocorre e a sua relação com os casos.

4.3.1. Setor público

Nas notas técnicas analisadas, há uma interação da Senacon com autoridades públicas nacionais e internacionais. Tendo em vista a competência concorrente de atuação dos integrantes do SNDC, a Secretaria dialoga principalmente com outras organizações que o integram, como Procons, Ministério Público e organizações da sociedade civil de defesa do consumidor.

Com relação aos Procons, a interação ocorreu nos casos relacionados ao uso indevido de dados de idosos para fins de telemarketing e venda de empréstimo consignado por instituições financeiras, em que a Superintendência do Procon do Estado do Tocantins e o Procon do Estado do Paraná juntaram ofícios relacionados a processos administrativos que instauraram com objeto semelhante em face das instituições financeiras representadas.

Ainda no escopo de organizações públicas que compõem o SNDC, é relevante a interação com Ministérios Públicos, em especial o Ministério Público do Distrito Federal e Territórios. Conforme mencionado anteriormente[61], o MPDFT foi uma autoridade que teve protagonismo em investigações envolvendo dados pessoais. Nesse sentido, não surpreende que em diversos casos as empresas representadas enfrentavam investigações concomitante na Senacon e na Unidade Especial de Proteção de Dados e Inteligência Artificial (Espec) do MPDFT. Casos concomitantes foram identificados nas investigações da C&A (sobre suposta comercialização de dados de consumidores); do Google (sobre o uso de dados para direcionamento de publicidade infantil no YouTube); do Facebook (sobre o escândalo do *Cambridge Analytica* e em outro sobre um ataque

[61] *Vide* nota 5.

hacker sofrido pelo Facebook); da Netshoes (sobre vazamento de dados de consumidores); e da Sky (sobre vazamento de dados de consumidores). Nessa interlocução, houve casos de maior (C&A e Netshoes) e menor (Google, Facebook e Sky) interação entre a Secretaria e o MPDFT.

No procedimento da C&A, o MPDFT enviou à Senacon cópia da Promoção de Arquivamento do Inquérito Civil Público 08190.029507/19-13, que havia instaurado para a investigação do caso, tendo em vista a adoção de medidas pela C&A para apuração e adoção de medidas corretivas ao incidente. O arquivamento do inquérito do MPDFT fez com que a Senacon também decidisse pelo arquivamento da averiguação preliminar que conduzia sobre a ocorrência.

Outra situação de maior interação foi o caso da Netshoes, em que a celebração de Termo de Ajustamento de Condutas entre o MPDFT e a empresa (TAC nº 01/2019), com a previsão de pagamento de indenização de danos morais coletivos em 500 mil reais, bem como o comprometimento da empresa em adotar um Programa de Proteção de Dados, fez com que a Secretaria arquivasse a Averiguação, tendo em vista o exaurimento de finalidade do caso ante o desfecho no âmbito do inquérito.

No caso do Google, a Senacon apenas cita na nota técnica pública a existência de procedimento com objeto semelhante tramitando como inquérito civil público perante o MPDFT (instaurado pela Portaria 4/2018). No caso do Facebook, a Secretaria menciona na averiguação preliminar a existência de abertura de inquérito civil público pelo MPDFT (por meio da Portaria 02/2018) e indica na decisão do processo administrativo que, a despeito de ter enviado Ofício ao MPDFT, não recebeu resposta ao pedido de informações sobre o andamento do inquérito. E, por fim, no caso da Sky, a Secretaria apenas menciona na nota técnica a homologação da promoção de arquivamento do inquérito civil público (instaurado pela Portaria 30/2018) no âmbito do MPDFT.

Com relação ao Ministério Público, houve também a averiguação preliminar em face do Google sobre *screening* (monitoramento) de e-mails do aplicativo Gmail, que foi aberta pela Senacon após a representação por meio de ofício da Procuradoria do Piauí do MPF. Vale ressaltar que, em entrevista com o servidor da Secretaria, foi dito que, nos casos de dificuldade comprobatória, os processos podem ser fortalecidos por meio de uma atuação mais próxima com o Ministério Público, "que pode atuar de forma mais enfática se for preciso".

Além das organizações que compõem o SNDC, a Secretaria também interagiu com outras entidades do setor público no âmbito das investigações, com a finalidade de obter informações técnicas de "órgãos peritos". Nesse mesmo caso do Google sobre *screening* de e-mails, a Senacon

consultou o Comitê Gestor da Internet no Brasil (CGI.br) sobre a possibilidade de o tratamento de dados ter sido realizado por um ser humano (e não por sistemas automatizados) e sobre a capacidade da tecnologia de realizar a reidentificação indireta de uma pessoa (anulando processos de anonimização). Em resposta, o CGI.br sustentou que a fiscalização não está entre as suas competências, apresentando parecer eminentemente jurídico (e não técnico), no qual, dentre outros argumentos, mencionava que "a privacidade é condição para o pleno exercício do direito de acesso à internet, sendo nulas aquelas cláusulas contratuais que viriam a transgredir a inviolabilidade e sigilo das comunicações privadas" (2019, p. 2).

Outro órgão com quem a Senacon interagiu de forma consultiva foi o Denatran, no caso da Mercedes-Benz, em que a Secretaria procurou o órgão para compreender se no seu processo de homologação de veículos haveria a obrigação de reporte sobre o uso de tecnologias, como o "e-call", que era objeto de questionamento na Europa, por ser um sistema de transmissão de dados e geolocalização de veículos utilizado para reapropriação de veículos de clientes inadimplentes. O Denatran respondeu ao Ofício da Secretaria, afirmando que não haveria a obrigação de reporte nos normativos vigentes no país.

Outra forma de interação da Secretaria foi no sentido de coletar dados e/ou evidências junto às bases de dados de entidades públicas. As autoridades públicas em que se constatou essa interação foram: Banco Central, INSS e Ministério da Economia.

A base de dados dos correspondentes do Banco Central foi consultada pela Secretaria para identificar a contratação de intermediadores de operações de empréstimos consignados (correspondentes) nos casos de investigação das instituições financeiras. O INSS foi oficiado pela Senacon para apresentar registros escritos de demandas registradas em seu sistema de ouvidoria sobre os mesmos casos. E, ainda nos casos das instituições financeiras, dados da ouvidoria do sistema "SOUWeb" do Ministério da Economia foram apresentados pelo Banco Safra para corroborar a tese de que a maioria das reclamações relacionadas à conduta investigada teriam sido decididas como improcedentes, no período de 2017 a 2019.

Outra forma de interação com autoridades públicas foi para fins de obtenção de informações de processos judiciais e/ou inquéritos policiais. A interação com a polícia ocorreu no caso da C&A, em que a Senacon oficiou a Polícia Federal em São Paulo e a Polícia Civil de São Paulo após receber a informação de que a empresa investigada teria apresentado notícia-crime ao tomar conhecimento das notícias sobre a comercialização ilegal de dados de clientes. A Corregedoria da

Polícia Federal respondeu ao Ofício da Secretaria, informando que declinou a competência para a apuração da notícia-crime, tendo encaminhado o protocolo à Polícia Civil do Estado de São Paulo para a adoção das providências cabíveis.

A interação com processos judiciais que estavam em andamento ocorreu em diferentes situações. Parte dessas situações esteve relacionada aos casos de investigação das instituições financeiras e o uso de dados de idosos, em que uma Ação Civil Pública (ACP), em face de uma correspondente bancária e do INSS, foi citada em diversas notas técnicas decisórias dos processos administrativos, inclusive tendo a Senacon emprestado prova da ACP para estabelecer o elo de responsabilidade solidária entre as empresas investigadas e a correspondente bancária que era ré na esfera judicial.

Outros casos em que processos judiciais discutiam fatos conexos ou idênticos aos procedimentos administrativos da Senacon ocorreram nas investigações do Google, sobre *screening* de e-mails; da Química Amparo, sobre vazamento de dados; e do Facebook, sobre o *Cambridge Analytica*. Nesses procedimentos, a menção aos processos judiciais foi pontual, não havendo grande interação da Secretaria com os seus documentos ou provas.

Finalmente, vale reiterar que a Senacon também menciona nas notas técnicas algumas autoridades estrangeiras, como o Federal Trade Commission (FTC) e o New York Attorney General's Office (NYAG). Com relação ao FTC, a Senacon iniciou procedimentos de ofício, adotando como justificativa a abertura de procedimentos de investigação pelo órgão americano. Vale ressaltar que a regulação da proteção de dados pessoais nos Estados Unidos é pulverizada entre as unidades federativas, não contando com uma autoridade regulatória específica ou uma legislação nacional e setorialmente transversal sobre o tema. Nesse cenário, o FTC, que é a Comissão Federal de Comércio americana, é quem atua com proeminência em casos envolvendo privacidade, quase como uma autoridade *ad hoc*, sendo o órgão responsável pela supervisão e fiscalização de normas setoriais de proteção de dados, como o COPPA (*Children's Online Privacy Protection Rule*).

O FTC foi mencionado no caso do Google sobre o uso de dados de menores para publicidade infantil no YouTube, tanto como justificativa da investigação, quanto como fundamento para decidir, tendo em vista o acordo que a empresa teria firmado com o órgão americano para melhor proteger os dados de crianças. Outro caso em que o FTC foi mencionado foi na averiguação preliminar e processo administrativo sobre o escândalo *Cambridge Analytica*,

do Facebook. Vale ressaltar que, neste último incidente, a Senacon empresta quase que integralmente a fundamentação adotada pelo FTC (e o depoimento de Mark Zuckerberg ao Congresso dos Estados Unidos) para sancionar o Facebook no âmbito do processo administrativo que conduzia.

De forma semelhante ao FTC, a abertura de investigação da plataforma Zoom pelo NYAG também foi citada como fator que teria ensejado a abertura de investigação pela Senacon. Vale ressaltar que o Zoom se comprometeu a adotar o mesmo nível de práticas de privacidade e de segurança da informação oferecidas aos usuários americanos decorrentes do acordo feito pela empresa com a NYAG (Procuradoria-Geral do Estado de Nova Iorque).

4.3.2. Setor privado

As organizações do setor privado com quem a Senacon dialoga nas notas técnicas são de dois tipos: empresas de comunicação e mídia e empresas de auditoria. Com relação aos portais de notícia, certas averiguações preliminares analisadas foram iniciadas de ofício pela Secretaria, após a verificação de indícios de violação às normas de defesa do consumidor nos eventos narrados pelos canais de notícia TechTudo (caso da Sky, sobre vazamento de dados), Jornal Globo (caso sobre a transcrição de áudios do Messenger pelo Facebook) e TecMundo (caso da J&A Holding, sobre comercialização de dados, e caso da Hering, sobre o uso de tecnologia de reconhecimento facial).

Nesse cenário, é interessante notar que a Senacon atua de forma reativa às notícias veiculadas em canais de comunicação e mídia especializados em segurança da informação e proteção de dados, abrindo investigações para apurar os casos com repercussão midiática. Outro ponto de interesse é que, em todos os casos em que a Secretaria abriu investigação com base em uma notícia, o fez por meio de averiguação preliminar, para avaliar se os indícios narrados nas matérias jornalísticas de fato apresentariam elementos suficientes para a instauração de processo administrativo sancionador.

Com relação às empresas de auditoria, não é raro que, após reunião presencial com as empresas investigadas, a representada apresente relatório de auditoria realizado por empresas de auditoria ou consultoria independentes sobre o evento investigado. Na entrevista com o servidor, foi possível saber que uma das maiores limitações institucionais do órgão se relaciona com a

capacidade técnica para a produção e análise de prova, especialmente quando os casos envolvem temas que exigem um alto nível de expertise em sistemas da informação. E, por esse motivo, era comum que nas reuniões a Secretaria sugerisse aos representados a apresentação de relatório produzido por essas empresas analisando o impacto e a gravidade dos incidentes de informação.

Nos termos da entrevista com o servidor da Secretaria:

> Eu não me recordo se a Senacon fazia um requerimento expresso dessas auditorias, mas sempre que as empresas apresentavam, era muito bem visto e (...) costumava ser sugerido porque na Senacon (...), por mais técnico que seja o órgão, e tem muitos servidores bons de carreira, e mesmo pessoas que não são concursadas são muito sérias lá dentro, (...) infelizmente é um órgão que está alocado no Executivo e, por estar no Executivo, existe uma pressão muito forte às vezes lá dentro. E muitas vezes é necessário tomar alguma medida com base numa notícia de jornal, e daí vem uma investigação. Um fato público e daí nasce um processo. Mas não é suficiente, então por isso que é tão importante que as empresas colaborem também durante as investigações.

É interessante a forma encontrada pela Secretaria para contornar as suas limitações em relação à capacidade institucional para a análise dos eventos investigados. Contudo, tendo em vista que essas empresas costumam ser custeadas pelas empresas investigadas, vale questionar a imparcialidade dos relatórios apresentados ou então a efetividade de implementação dos planos de resposta apresentados[62].

4.3.3. Terceiro Setor

As organizações do Terceiro Setor de defesa do consumidor compõem o SNDC. Vale ressaltar que, nos casos estudados, interagem a Senacon e/ou organizações nacionais e internacionais da sociedade civil, como o IDEC, a SOS Consumidor, o Instituto de Defesa Coletiva, o DefConLab, a Eletronic Frontier Foundation e a Privacy International.

O IDEC, como integrante do SNDC, por vezes foi o órgão que provocou a Secretaria a instaurar os procedimentos administrativos, apresentando representações à Senacon contra as empresas representadas. Isso ocorreu no caso da Hering, sobre o uso de tecnologia de reconhecimento facial. Vale ressaltar que o pano de fundo da discussão do caso Hering envolveu o uso de tecnologia de reconhecimento facial para a finalidade de direcionamento de marketing, bem como os limites da anonimização quando há o uso desse tipo de tecnologia. Tema que também

[62] Sobre o ponto da imparcialidade, vale ressaltar que essa foi uma reflexão feita após a conclusão da entrevista, não tendo o entrevistado se posicionado sobre esse tema.

esteve presente em outro litígio estratégico do IDEC, na Ação Civil Pública contra a Via Quatro Amarela, que tramitou perante o Tribunal de Justiça do Estado de São Paulo, em que o IDEC foi vitorioso em primeira e segunda instâncias. Vale dizer que o precedente judicial da Via Quatro foi citado pela Senacon nos casos que discutiam os limites da anonimização, que será mais bem abordado na seção seguinte deste trabalho.

Outros incidentes que surgiram por representação do IDEC foram frutos de uma parceria desta organização com o Instituto de Defesa Coletiva. Esses casos foram as investigações das instituições financeiras sobre o uso indevido de dados de idosos na oferta de empréstimo consignado. Sobre a relação do IDEC com a Senacon, o entrevistado relatou o seguinte:

> O IDEC, ele tem uma força grande na Senacon, porque o IDEC participa de conselhos na Senacon, ele tem uma proximidade com a Secretaria, muitas vezes ele questiona a atuação da Secretaria quando ele discorda de posicionamentos (...) não necessariamente o que o IDEC denuncia vai ser punido. Vai ser investigado, existe uma defesa do contraditório (...). Então, assim, (...) apesar da força que eles têm, de participar da Secretaria de uma forma mais ativa, não existe nenhum tipo de influência no sentido de "isso aqui veio do IDEC então essa decisão já está contaminada". Não, muito pelo contrário, acho que o cuidado é redobrado.

A SOS Consumidor é citada na averiguação preliminar do Facebook sobre o caso *Cambridge Analytica*, uma vez que a organização propôs Ação Civil Pública em face da empresa investigada, pedindo a condenação do pagamento de indenização por danos morais coletivos ao Facebook em decorrência do compartilhamento indevido de dados de usuários. O objeto da ACP proposta pela SOS Consumidor, de acordo com a Senacon, era "verificar as circunstâncias do vazamento e do mal uso de dados dos usuários do Facebook, bem como da conduta da empresa Facebook, que, segundo a petição inicial respectiva, não teria sido suficiente para impedir que algumas ferramentas da sua plataforma fossem usadas para roubar dados".

O Def ConLab é um laboratório de pesquisa sem fins lucrativos, que tem por objetivo produzir dados sobre vulnerabilidades, ameaças cibernéticas, riscos cibernéticos e *big data*. A veiculação de artigo no *site* sobre o "Vazamento de Dados – Robinhood", que denunciava que certas empresas privadas estavam comercializando dados pessoais, inclusive financeiros, de brasileiros, sendo uma delas a J&A Holding e as suas empresas subsidiárias, fez com que a Secretaria instaurasse averiguação preliminar contra a Holding.

A *Eletronic Frontier Foundation* (EFF) é uma organização americana da sociedade civil sem fins lucrativos, que atua desde 1990 em prol dos direitos digitais, em especial os direitos à

privacidade e à liberdade de expressão[63]. A EFF é mencionada pela Senacon no caso da plataforma Zoom, sobre as falhas de segurança, em que a organização teria feito uma declaração na matéria de jornal que ensejou a instauração da averiguação preliminar indicando

> (...) que os hosts das chamadas de Zoom podem ver se os participantes têm a janela Zoom aberta ou não, o que significa que eles podem monitorar se as pessoas provavelmente estão prestando atenção. Os administradores também podem ver o endereço IP, os dados de localização e as informações do dispositivo em cada participante.

Por fim, a *Privacy International* é uma organização inglesa da sociedade civil sem fins lucrativos que atua desde 1990 na promoção do direito humano à privacidade. A organização é citada no caso da Mercedes-Benz sobre o uso de tecnologia de "e-call" na Europa para localização de carros de clientes inadimplentes. A Senacon cita uma declaração da *Privacy International* na qual afirma que "o que a Mercedes está a fazer é tecnicamente ilegal", tendo em vista que a legislação aprovada pelo Parlamento Europeu que obrigava a implementação do "e-call" em todos os veículos comercializados na União Europeia seria destinada a "situações de emergência, em caso de acidente grave e limitava-se a comunicar dados básicos (tipo de veículo, combustível, hora do acidente, número de passageiros e a localização do carro)".

4.4. Os dispositivos violados

A seguir, apresentamos a relação de dispositivos utilizados pela Senacon para decisão das averiguações preliminares e processos administrativos de sanção:

Tabela 1 – Dispositivos aplicados pela Senacon na fundamentação das decisões

Lei	Dispositivo	Texto
CDC	Art. 4º, *caput*	Art. 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios:
CDC	Art. 4º, I	I – reconhecimento da vulnerabilidade do consumidor no mercado de consumo;
CDC	Art. 4º, III	III – harmonização dos interesses dos participantes das relações de consumo e compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico, de modo a viabilizar os princípios nos

[63] Informações sobre a EFF disponíveis em: https://www.eff.org/about/history. Acesso em: 5 dez. 2021.

		quais se funda a ordem econômica (art. 170, da Constituição Federal), sempre com base na boa-fé e equilíbrio nas relações entre consumidores e fornecedores;
CDC	Art. 4º, IV	IV – educação e informação de fornecedores e consumidores, quanto aos seus direitos e deveres, com vistas à melhoria do mercado de consumo;
CDC	Art. 6º, II	[Art. 6º São direitos básicos do consumidor:] II – a educação e divulgação sobre o consumo adequado dos produtos e serviços, asseguradas a liberdade de escolha e a igualdade nas contratações;
CDC	Art. 6º, III	III – a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem;
CDC	Art. 6º, IV	IV – a proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços;
CDC	Art. 6º, VI	VI – a efetiva prevenção e reparação de danos patrimoniais e morais, individuais, coletivos e difusos;
CDC	Art. 14	Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos. § 1º O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais: I – o modo de seu fornecimento; II – o resultado e os riscos que razoavelmente dele se esperam; III – a época em que foi fornecido. § 2º O serviço não é considerado defeituoso pela adoção de novas técnicas. § 3º O fornecedor de serviços só não será responsabilizado quando provar: I – que, tendo prestado o serviço, o defeito inexiste; II – a culpa exclusiva do consumidor ou de terceiro. § 4º A responsabilidade pessoal dos profissionais liberais será apurada mediante a verificação de culpa.
CDC	Art. 18	Art. 18. Os fornecedores de produtos de consumo duráveis ou não duráveis respondem solidariamente pelos vícios de qualidade ou quantidade que os tornem impróprios ou inadequados ao consumo a que se destinam ou lhes diminuam o valor, assim como por aqueles decorrentes da disparidade, com a indicações constantes do recipiente, da embalagem, rotulagem ou mensagem publicitária, respeitadas as variações decorrentes de sua natureza, podendo o consumidor exigir a substituição das partes viciadas.

		§ 1º Não sendo o vício sanado no prazo máximo de trinta dias, pode o consumidor exigir, alternativamente e à sua escolha: I – a substituição do produto por outro da mesma espécie, em perfeitas condições de uso; II – a restituição imediata da quantia paga, monetariamente atualizada, sem prejuízo de eventuais perdas e danos; III – o abatimento proporcional do preço.
CDC	Art. 31	Art. 31. A oferta e apresentação de produtos ou serviços devem assegurar informações corretas, claras, precisas, ostensivas e em língua portuguesa sobre suas características, qualidades, quantidade, composição, preço, garantia, prazos de validade e origem, entre outros dados, bem como sobre os riscos que apresentam à saúde e segurança dos consumidores. Parágrafo único. As informações de que trata este artigo, nos produtos refrigerados oferecidos ao consumidor, serão gravadas de forma indelével.
CDC	Art. 37	Art. 37. É proibida toda publicidade enganosa ou abusiva. § 1º É enganosa qualquer modalidade de informação ou comunicação de caráter publicitário, inteira ou parcialmente falsa, ou, por qualquer outro modo, mesmo por omissão, capaz de induzir em erro o consumidor a respeito da natureza, características, qualidade, quantidade, propriedades, origem, preço e quaisquer outros dados sobre produtos e serviços. § 2º É abusiva, dentre outras a publicidade discriminatória de qualquer natureza, a que incite à violência, explore o medo ou a superstição, se aproveite da deficiência de julgamento e experiência da criança, desrespeita valores ambientais, ou que seja capaz de induzir o consumidor a se comportar de forma prejudicial ou perigosa à sua saúde ou segurança. § 3º Para os efeitos deste código, a publicidade é enganosa por omissão quando deixar de informar sobre dado essencial do produto ou serviço.
CDC	Art. 39, *caput*	Art. 39. É vedado ao fornecedor de produtos ou serviços, dentre outras práticas abusivas:
CDC	Art. 39, IV	IV – prevalecer-se da fraqueza ou ignorância do consumidor, tendo em vista sua idade, saúde, conhecimento ou condição social, para impingir-lhe seus produtos ou serviços;
CDC	Art. 43	Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

		§ 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. § 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. § 5º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. § 6º Todas as informações de que trata o *caput* deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.
CDC	Art. 52	Art. 52. No fornecimento de produtos ou serviços que envolva outorga de crédito ou concessão de financiamento ao consumidor, o fornecedor deverá, entre outros requisitos, informá-lo prévia e adequadamente sobre: I – preço do produto ou serviço em moeda corrente nacional; II – montante dos juros de mora e da taxa efetiva anual de juros; III – acréscimos legalmente previstos; IV – número e periodicidade das prestações; V – soma total a pagar, com e sem financiamento.
CDC	Art. 88	Art. 88. Na hipótese do art. 13, parágrafo único deste código, a ação de regresso poderá ser ajuizada em processo autônomo, facultada a possibilidade de prosseguir-se nos mesmos autos, vedada a denunciação da lide.
MCI	Art. 2º, II	[Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:] II – os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
MCI	Art. 2º, III	III – a pluralidade e a diversidade;
MCI	Art. 7º, I	[Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:] I – inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
MCI	Art. 7º, VI	VI – informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
MCI	Art. 7º, VII	VII – não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

MCI	Art. 7º, VIII	VIII – informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
MCI	Art. 7º, IX	IX – consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
MCI	Art. 7º, X	X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;
MCI	Art. 7º, XIII	XIII – aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.
MCI	Art. 10, *caput*	Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
MCI	Art. 10, § 1º	§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no *caput*, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º .
MCI	Art. 11	Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. § 1º O disposto no *caput* aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil. § 2º O disposto no *caput* aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil. § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao

	armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações. § 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Fonte: autoria própria

Vale ressaltar que a Senacon não utiliza a LGPD como fundamento das decisões dos procedimentos administrativos, mesmo nas decisões após a entrada em vigor da lei (em agosto de 2020). De acordo com o servidor entrevistado: "isso era proposital: não pautava tanto na lei de proteção de dados pra evitar eventuais conflitos futuros com a ANPD".

E, nesse mesmo sentido:

> Minha opinião: eu acho que a Senacon vai continuar atuando com base no CDC, e é proposital que eles não mencionem a LGPD ou o GDPR nas notas técnicas justamente para evitar qualquer conflito porque de fato o CDC protege também o consumidor no âmbito dos dados. Mas existe um grande questionamento jurídico em cima disso. Até que ponto é uma dupla punição de um mesmo fato, vamos ver como o Judiciário vai enxergar, o que vai vir daqui pra frente...

Com relação à utilização de princípios e direitos básicos na fundamentação das decisões, o entrevistado comentou que se trata de uma estratégia que antecipa eventual judicialização das decisões administrativas tomadas pela Secretaria:

> Muitas vezes os princípios são o melhor caminho porque eles resguardam quem está escrevendo, mostram motivação de uma forma mais ampla. E existe todo um cuidado também com o que vem depois da decisão porque muitas empresas vão judicializar. Eu imagino que esses casos de proteção de dados, é inevitável, vai para o Judiciário a partir do momento que tiver uma sanção significativa. E as investigações continuam, e eu imagino que o que vem aí de questionamento é justamente esse ponto que você colocou numa das perguntas sobre a competência. Então é realmente um excesso de cuidado que existe lá dentro. A gente sabe que muitas vezes as notas técnicas deixam portas abertas, mas nem sempre é possível fechar justamente por essa dificuldade de gente. É uma Secretaria muito pequena, com um quadro de servidores reduzido.

Concluindo, a presente Seção teve por objetivo apresentar uma visão geral dos casos estudados, por meio da descrição em quatro partes: (i) a Senacon e o DPDC; (ii) os casos investigados; (iii) os atores com quem a Senacon interage; e (iv) os dispositivos jurídicos mobilizados pela Secretaria para fundamentar as decisões das notas técnicas. Essa parte descritiva teve por objetivo apresentar o contexto e os aspectos gerais dos casos para, na Seção seguinte, aprofundar a análise das "palavras-chave" que traduzem a "gramática" adotada pela Senacon.

5. PALAVRAS-CHAVE: A PROTEÇÃO DE DADOS PESSOAIS NA SECRETARIA NACIONAL DO CONSUMIDOR

A estrutura desta seção se inspira na obra *Keywords: a vocabulary of culture and society* (1983), do acadêmico gaulês Raymond Williams, um dos exponentes da Nova Esquerda inglesa. Com o fim da Segunda Guerra Mundial, Williams recebeu baixa do exército inglês e teve a oportunidade de retomar os seus estudos em Cambridge, que foram suspensos pelos quatro anos e meio em que ele esteve na guerra.

Ao retornar a Cambridge, Williams estranhou que "as pessoas simplesmente não falavam a mesma língua" (2007, p. 27), fazendo referência à ideia de que, aparentemente, os seus colegas não compartilhavam mais os mesmos valores semânticos que ele a determinados conceitos. Essa percepção sobre a mudança de sentido conceitual é evidenciada na palavra *cultura*, fenômeno que Williams atribui a possíveis mudanças sociais (especialmente nas esferas da política e da religião) impulsionadas pela Revolução Industrial e seus desdobramentos até o segundo pós-guerra.

A partir dessa percepção, Williams constrói uma definição histórico-linguística para verbetes considerados centrais pelo autor na cultura e vida social de sua época, como "arte" e "sociedade". A presente pesquisa se inspira no trabalho de Williams de duas maneiras. A primeira, em relação à forma de compreender a língua e suas palavras como resultado de um processo social e histórico, em que seu significado depende do contexto em que surgem e como são efetivamente utilizadas. A segunda, em termos de estrutura, adotando a ordem alfabética para trabalhar os significados dos conceitos.

Conceitos jurídicos são formados a partir de processos sociais, históricos e institucionais. Após quase uma década de debates legislativos, uma Lei Geral de Proteção de Dados Pessoais é sancionada em um ordenamento jurídico que já dispunha de regulações esparsas e setoriais sobre o tema. Nesse sentido, a pesquisa busca analisar conceitos a partir de um determinado contexto, isto é, investigar como uma parte do arranjo brasileiro de proteção de dados preexistente à LGPD tem se relacionado com as regras, princípios e pressupostos normativos dessa lei. Ainda que a proteção de dados pessoais brasileira "nos livros" aparente uma grande influência dos debates internacionais de regulação da proteção de dados, em especial o europeu, esta pesquisa aborda os conceitos "em ação", para capturar como a Senacon, um órgão local que gestou o anteprojeto que

daria origem à LGPD, tem mobilizado o Direito para interpretar e decidir casos de "uso indevido de dados" de consumidores.

Com relação ao segundo ponto de inspiração em Williams, ainda que a ordem alfabética possa não realçar as relações intrínsecas de determinados conceitos, qualquer outro tipo de estrutura (como a organização por áreas ou temas) estabeleceria um conjunto de conexões entre categorias conceituais, ao mesmo tempo que suprimiria outro. Nesse sentido, a ordem alfabética, com o uso de referências cruzadas, permite ao leitor uma leitura imediata mais fácil, apta a estabelecer outros tipos de conexão e comparação a partir da integralidade do texto (2007, p. 44).

Assim, esta seção tem por objetivo a construção da "gramática" adotada pela Secretaria Nacional do Consumidor a partir da identificação das "palavras-chave", isto é, as categorias conceituais que traduzem a forma como a Senacon aplica o Direito nas decisões analisadas. Os conceitos aqui expostos partem do exercício de codificação das notas técnicas e do posterior agrupamento dos códigos de sentido semelhante em categorias conceituais, capturando as suas propriedades e dimensões a partir dos dados analisados (notas técnicas e entrevista). Em cada conceito, a pesquisa analisa a relação entre a abordagem da Senacon à proteção de dados pessoais e os conceitos, regras e pressupostos normativos advindos da LGPD (Lei n. 13.709/2018).

5.1. Agentes de tratamento

A LGPD define a expressão "agentes de tratamento" como o conjunto de controladores e operadores de dados pessoais (art. 5º, IX, da LGPD). De acordo com a LGPD, "controlador" é a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (art. 5º, VI, da LGPD). Por sua vez, o "operador" é definido como a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (art. 5º, VII, da LGPD).

A legislação cria essas três categorias para diferenciar a forma que distribui obrigações legais e responsabilidades a cada agente de tratamento, conforme agência e ingerência na cadeia de tratamento de dados pessoais. Nesse sentido, existem dispositivos da LGPD que são direcionados igualmente a controladores e operadores de dados pessoais – situação em que a lei adota a definição conjunta de "agentes de tratamento". Por outro lado, existem outras situações em que obrigações e responsabilidades específicas são direcionadas ora àqueles que tomam as decisões

referentes ao tratamento de dados pessoais[64] (os "controladores" de dados pessoais), ora àqueles que realizam as operações de tratamento de dados para o controlador dos dados pessoais, em seu nome[65] (os "operadores" de dados pessoais).

Na LGPD, a articulação dessas categorias é especialmente relevante para a responsabilização dos agentes de tratamento por eventual dano aos titulares dos dados pessoais. Nos termos da lei, o agente de tratamento "que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo" (art. 42, *caput*, da LGPD). Nesses casos, respondem de forma solidária (i) o operador que "descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador" (art. 42, I, da LGPD), e (ii) outros controladores "diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados" (art. 42, II, da LGPD).

A isenção de responsabilidade do agente de tratamento pelo dano causado ao titular de dados ocorre nas seguintes situações: (i) quando o agente comprova que não realizou o tratamento de dados pessoais (art. 43, I, da LGPD); (ii) quando o agente comprova que não houve violação à legislação de proteção de dados (art. 43, II, da LGPD); (iii) quando o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros (art. 43, III, da LGPD).

Em todos os procedimentos administrativos analisados no escopo da pesquisa, as empresas investigadas pela Senacon poderiam ser classificadas, de acordo com a LGPD, como controladoras de dados pessoais. Nesse cenário, em alguns casos, a estratégia adotada pela empresa investigada foi demonstrar a culpa de um terceiro prestador de serviço (operador de dados pessoais) ou de outros controladores de dados pessoais pelo "uso indevido de dados".

Os casos em que a empresa investigada teria atribuído a um terceiro "operador" de dados a culpa pelo dano foram os da Tim[66] e Sky[67]. No caso da Tim, uma plataforma contratada pela empresa para operacionalizar a renegociação de dívidas de clientes teria vazado dados pessoais, incluindo informações financeiras (como dívidas em aberto). A defesa da Tim envolveu alegar que

[64] Exemplo: "Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei" (art. 8º, § 2º, da LGPD).
[65] Exemplo: "O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria" (art. 39 da LGPD).
[66] Processo Administrativo nº 08012.001392/2019-15.
[67] Processo Administrativo nº 08012.003074/2018-16.

o desenvolvimento da plataforma teria sido terceirizado por uma outra empresa, denominada Grupo Services. Em relação ao incidente, a empresa terceirizada teria concluído que "o ambiente em que o timnegocia.com.br encontra-se hospedado" teria sido "objeto de ação criminosa". A Tim também alegou que o contrato firmado entre ela e a Grupo Services disporia de cláusula no sentido da responsabilização integral da terceirizada por "qualquer prejuízo que acarretasse à TIM ou a terceiros, bem como eventuais deveres de reparação (...)".

Na nota técnica de decisão do processo administrativo, diante dos argumentos de que a Grupo Services seria a responsável pelo vazamento, a Secretaria se posicionou no seguinte sentido:

> Em que pese a alegação da Representada de que a plataforma seria terceirizada, o consumidor que acessava o site tinha a relação de consumo com a Representada, tendo em vista que a renegociação de dívidas seria com ela. Entende-se que a relação estabelecida entre o fornecedor de acesso à internet e/ou conteúdo e o usuário é objeto de análise do Direito do Consumidor. No presente processo, o usuário desconhecia qualquer terceirização da plataforma, de modo que é necessário analisar o direito à proteção digital do consumidor pela Representada. (2019, p. 2)

O fundamento legal da Secretaria foi de que o art. 88 do CDC estabeleceria vedação expressa da denunciação à lide nas relações de consumo, sendo possível aplicar a responsabilidade objetiva nos casos de dano aos consumidores (art. 14 do CDC). Contudo, fosse o caso analisado pelas lentes da LGPD, a Tim poderia eventualmente ter recorrido a uma das hipóteses de isenção de responsabilidade tratadas anteriormente (art. 42 da LGPD).

Outro caso em que a culpa de um terceiro "operador" de dados foi suscitada pela empresa investigada ocorreu na averiguação preliminar contra a Sky, em que dados de 32 milhões de consumidores teriam ficado expostos nos servidores da Amazon ante um erro de configuração. A defesa da Sky, suportada pela consultoria *PricewaterhouseCoopers (PwC)*, foi no sentido de que o incidente teria sido uma "exposição temporária de dados" que "se deu por conta de erro de configuração de armazenamento do servidor da ElasticSearch da AWS, ocasionada por um terceiro contratado" e que apenas poderia ser acessada por "pessoa com conhecimento tecnológico avançado".

Nesse caso, a discussão sobre a responsabilidade do terceiro contratado pela Sky para configuração do serviço *Elastic Search* de hospedagem de dados nos servidores da AWS não foi enfrentada, ainda que tenha sido invocada pela Sky. Com o apoio da *PwC*, a Sky montou um relatório detalhado de investigação e plano de resposta ao incidente, o que fez com que a Secretaria

entendesse que a empresa teria tomado medidas reparatórias necessárias, aptas a garantir a proteção do consumidor e, por isso, a finalidade do procedimento administrativo teria se exaurido.

Em outros casos, a relação entre as empresas investigadas e terceiros poderia ser classificada pela LGPD como uma relação entre controladores de dados pessoais, uma vez que tanto a investigada quanto o terceiro teriam autonomia para tomar decisões sobre o tratamento de dados pessoais. Esses casos envolveram dois procedimentos administrativos contra o Facebook e dez procedimentos administrativos contra instituições financeiras.

Os casos do Facebook envolveram o compartilhamento de dados de usuários com terceiros desenvolvedores de aplicativos. Em ambos, o Facebook buscou argumentar que a responsabilidade pelo uso indevido de dados seria desses terceiros. No caso *Cambridge Analytica*[68], Aleksander Kogan, um cientista de dados e pesquisador na área dos estudos comportamentais, teria desenvolvido um aplicativo denominado "This is Your Digital Life", que consistia em um quiz de personalidade que utilizava o recurso Facebook Login para autenticação de usuários da plataforma em seu aplicativo. Aqueles que acessaram o aplicativo de Kogan por meio da ferramenta de Facebook Login entre 2013 e 2015 tiveram os seguintes dados compartilhados: "a) dados do perfil público, incluindo nome e gênero; b) data de nascimento; c) 'cidade atual' indicada na seção sobre perfil do usuário, se informada; d) páginas que o usuário curtiu; e) lista de amigos e, quanto a estes, as mesmas informações acima" (2019, p. 2). A prática de compartilhamento de dados de usuários e dos amigos de usuários fez com que aproximadamente 443.000 usuários do Facebook tivessem seus dados compartilhados com o aplicativo do pesquisador Aleksander Kogan.

Ocorre que Kogan teria transferido os dados dos usuários para outra empresa denominada *Cambridge Analytica* (controlada pela empresa SCL Elections Limited), que teria utilizado essas informações para outras finalidades, dentre as quais, a de marketing político. A defesa do Facebook foi no sentido de responsabilizar Aleksander Kogan e a *Cambridge Analytica* pelo uso indevido de dados, tendo em vista que referido compartilhamento violaria os termos e as condições da plataforma voltada a desenvolvedores de aplicativos. Nesse caso, a decisão da Senacon prescindiu da análise de responsabilidade de Aleksander Kogan e da *Cambridge Analytica* pelo uso indevido de dados, entendendo que a prática abusiva do Facebook teria ocorrido pelo seu próprio modelo de negócios, que falhou nos deveres: de informar os usuários sobre o compartilhamento de dados de

[68] Processo nº 08012.000723/2018-19 (averiguação preliminar); Processo nº 08012.000723/2018-19 (processo administrativo).

amigos, de coletar um consentimento específico para o compartilhamento de dados e de monitorar os desenvolvedores de aplicativos que utilizavam os recursos de compartilhamentos de dados da plataforma.

O segundo caso também envolveu desenvolvedores de aplicativos que usavam recursos de compartilhamento disponibilizados pela plataforma[69]. Nesse procedimento, dois aplicativos distintos, *Cultura Coletiva* (destinado a usuários mexicanos) e *At the Pool* (destinado a usuários norte-americanos), teriam armazenado "curtidas, comentários, fotos, músicas, informações sobre amigos, eventos e até reservas de voos e hotéis" em servidores da *Amazon Web Services* sem controles adequados de acesso a esses dados, expondo tais informações a acessos não autorizados. Nesse caso, o Facebook novamente salientou que a responsabilidade pelo armazenamento incorreto de informações seria de terceiros desenvolvedores de aplicativos. A averiguação preliminar acabou sendo arquivada ante a inexistência de indícios de que os incidentes teriam afetado consumidores brasileiros. De toda forma, na nota técnica de arquivamento do feito, a Senacon postulou o seguinte:

> Sob a égide de proteção deferida pelo Código de Defesa do Consumidor, independentemente do caso referir-se a uma exposição temporária de dados que não se realizou diretamente nos sistemas operacionais da plataforma do Facebook, o fato não exclui a responsabilidade do fornecedor com que o consumidor contratou originariamente, no caso o Facebook, visto que, independentemente do causador da exposição dos dados, os mesmos foram expostos. (2020, p. 4)

Nesse sentido, para a Senacon, haveria responsabilidade do Facebook por dano ocasionado por terceiro, sob o fundamento de a empresa ser o fornecedor com quem o consumidor teria contratado originalmente, não havendo a possibilidade de limitação de responsabilidade do Facebook por eventual culpa exclusiva de terceiro.

Por fim, nos casos das instituições financeiras, a discussão girou em torno da responsabilidade da Caixa Econômica Federal[70], do Safra[71], do Banco Olé[72], do Banco Itaú

[69] Processo nº 08012.001086/2019-89.
[70] Averiguação Preliminar Processo nº 08012.001492/2019-41.
[71] Averiguação Preliminar Processo nº 08012.001486/2019-94; Processo Administrativo nº 08012.001486/2019-94.
[72] Averiguação Preliminar Processo nº 08012.001483/2019-51.

Consignado[73], do Banrisul[74], do Banco Pan[75], do Banco Cetelem[76], do Banco Bradesco[77], do Banco BMG[78] e do Branco Bradesco Financiamentos[79] pelo uso indevido de dados de idosos por seus correspondentes bancários. Correspondentes bancários são intermediários que oferecem os produtos de instituições financeiras a consumidores finais, sendo significativa a utilização desse modelo de negócios na comercialização de empréstimos consignados, cujo público-alvo é predominantemente formado por aposentados e pensionistas do INSS.

Após ter recebido a notícia de um vazamento de uma base de dados do INSS e ter apurado o aumento de reclamações sobre telemarketing e publicidade abusiva na oferta de consignados a idosos no Sindec, a Senacon iniciou procedimentos administrativos contra as dez instituições financeiras que figuravam entre as que mais teriam recebido esse tipo de reclamação. De uma forma geral, a defesa das instituições financeiras foi no sentido de atribuir aos correspondentes bancários a responsabilidade por eventual uso indevido de dados, ressaltando que os correspondentes teriam sido orientados a "agir de maneira adequada, de forma a não infringir qualquer dispositivo legal".

Cetelem, Pan, Safra, BMG e Itaú Consignado tiveram decisões sancionatórias nos processos administrativos[80]. Quanto à responsabilidade das instituições pelos correspondentes bancários, ao sancioná-las, a Secretaria se baseou na falha das instituições de exercerem "diligentemente o seu dever de vigilância e de fiscalização das atividades realizadas pela correspondente bancária", tendo em vista "uma postura negligente no monitoramento de seus correspondentes (que nada mais eram que agentes *longa manus*, divulgando produtos e contratando em seu nome)". Assim, também no caso das instituições financeiras, a Senacon não teria admitido a tese de isenção de responsabilidade por culpa exclusiva de terceiro.

---

[73] Averiguação Preliminar Processo nº 08012.001470/2019-81; Processo Administrativo nº 08012.001470/2019-81.
[74] Averiguação Preliminar Processo nº 08012.001490/2019-52.
[75] Averiguação Preliminar Processo nº 08012.001462/2019-35; Processo Administrativo nº 08012.001462/2019-35.
[76] Averiguação Preliminar Processo nº 08012.001476/2019-59; Processo Administrativo nº 08012.001476/2019-59.
[77] Averiguação Preliminar Processo nº 08012.001489/2019-28.
[78] Averiguação Preliminar Processo nº 08012.001478/2019-48; Processo Administrativo nº 08012.001478/2019-4.
[79] Averiguação Preliminar Processo nº 08012.001488/2019-83.
[80] A Senacon não disponibilizou as notas técnicas conclusivas dos processos administrativos das demais instituições financeiras. Com as informações disponíveis, não é possível concluir se os demais casos chegaram a ter uma decisão conclusiva (sancionatória ou não).

Conforme exposto anteriormente, a LGPD criou as figuras do "controlador", do "operador" e de "agentes de tratamento" para distribuir obrigações legais, bem como para regular a forma de responsabilidade de cada agente na cadeia de tratamento de dados pessoais em caso de dano ao titular dos dados. Alguns dos procedimentos administrativos estudados no escopo da presente pesquisa se relacionavam com esses diferentes papéis na cadeia de tratamento, especialmente em termos de culpa para a ocorrência do "uso indevido de dados". Contudo, conforme se apreende da análise dos casos, a Senacon, em todos eles, adotou o pressuposto da responsabilidade objetiva do CDC, prescindindo de uma análise aprofundada sobre os diferentes papéis e a culpa de cada agente de tratamento pelo uso indevido de dados, a depender das circunstâncias concretas dos casos. Nesse sentido, a "gramática" protetiva da Senacon aplicada ao conceito de agentes de tratamento prescinde de uma análise sobre o papel da empresa na cadeia de tratamento, bem como a medida da sua culpa para o "uso indevido de dados", adotando como pressuposto a ideia de que a empresa é responsável, independentemente do seu papel.

5.2. Anonimização

A LGPD define o dado anonimizado como o "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (art. 5º, III, da LGPD) e a anonimização como a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo".

Em outras palavras, o processo de anonimização permite, com maior ou menor grau de intensidade (a depender da técnica implementada para a realização do processo), gerenciar circunstancialmente o grau de identificabilidade de uma dada base de dados (BIONI, 2020).

Trata-se de uma definição importante, ao passo que dados sujeitos ao processo de anonimização não estão dentro do escopo de aplicação da LGPD, salvo quando a anonimização puder ser revertida, usando exclusivamente meios próprios, ou com esforços razoáveis (art. 12, *caput*, da LGPD), ou quando os dados forem usados para a formação de perfil comportamental de determinada pessoa, se identificada (art. 12, § 2º, da LGPD). Nesse sentido, o dado anonimizado é o conceito antítese do dado pessoal. A consequência prática da anonimização é que as organizações

se tornam aptas para utilizar dados anonimizados para o desenvolvimento de pesquisas, novos projetos e produtos sem o ônus de cumprir com os demais requisitos previstos na LGPD.

Na Senacon, a discussão sobre anonimização foi central na averiguação preliminar e no processo administrativo do caso Hering[81]. De acordo com a nota técnica do processo administrativo, em 2019, a Hering teria inaugurado uma loja no Shopping Morumbi chamada *Hering Experience*, "que possuiria diversos recursos tecnológicos de personalização para o usuário. Na loja, os sistemas monitoram a reação de clientes às roupas por meio do reconhecimento facial, que seria, segundo a empresa, uma 'experiência' para a publicidade personalizada" (2020, p. 1). A Hering teria se manifestado no sentido de que "as soluções tecnológicas implementadas não realizavam qualquer tipo de reconhecimento facial, tampouco a individualização de consumidores; produziam apenas informações estatísticas sobre a loja e sobre o fluxo de pessoas que nela transitavam, de forma totalmente anonimizada" (2020, p. 2).

Para ilustrar seus argumentos, a Hering explicou à Senacon como as ferramentas de *Video Analytics* e *Digital Signage* instaladas na loja eram utilizadas. De acordo com a empresa, a primeira era usada para análise e "produção de mapas de calor com o intuito de indicar os pontos mais frequentados da loja, bem como estimativa de gênero, faixa etária e humor dos consumidores no ambiente da loja, a partir da detecção facial feita por uma única câmera instalada próximo ao caixa da loja, para contar as pessoas e produzir relatórios estatísticos" (2020, p. 2). A Hering argumentou, ainda, que as informações coletadas eram utilizadas para "medir a circulação interna na loja, dias e horários de maior pico, bem como áreas de maior interesse dos consumidores" (2020, p. 8), reiterando que "todas as estimativas geradas a partir dos dados estatísticos tratados eram de baixa precisão" (2020, p. 8). Com relação à ferramenta de *Digital Signage*, a Hering explicou que era empregada para otimizar "a transmissão de conteúdo publicitário no ambiente daquela loja, com direcionamento de campanhas a partir da classificação de gênero, de maneira anonimizada e, posteriormente, na medição estatística da audiência" (2020, p. 3).

Essa diferença que a Hering busca trabalhar na sua defesa administrativa entre "reconhecimento facial" e "detecção facial" é uma tentativa de argumentar que os dados utilizados pelas ferramentas empregadas pela loja tratavam os dados de forma anonimizada. A empresa também argumenta de forma pragmática, sustentando que, além de não ser possível a identificação

[81] Averiguação Preliminar Processo nº 08012.001387/2019-11; Processo Administrativo nº 08012.001387/2019-11.

de consumidores, a tecnologia não permitiria "capturar, armazenar dados pessoais ou utilizar essas informações para o envio de mensagens direcionadas aos consumidores individualizados" (2020, p. 3). Nesse sentido, a Hering buscava construir a tese de que tratava dados anonimizados tanto por limitações da tecnologia quanto por uma análise consequencial em relação ao seu uso (que não seria individualizado ou com efeitos sobre os indivíduos).

Ao decidir o processo administrativo, a Senacon classificou a conduta da Hering como "utilização de tecnologia para a coleta de dados de consumidores sem conhecimento prévio e consentimento, como consequente ofensa ao direito básico do consumidor" (2020, p. 6), no sentido do trecho exposto a seguir:

> Embora a representada argumente no sentido de que as soluções tecnológicas implementadas não realizavam qualquer tipo de reconhecimento facial, tampouco a individualização de consumidores, mas que apenas produziam informações estatísticas sobre a loja e sobre o fluxo de pessoas que nela transitavam, de forma totalmente anonimizada, fato é que os consumidores tinham o direito de saber, ao menos, o que estava acontecendo. Assim, a representada, nitidamente, aproveitou-se não só da vulnerabilidade, mas também da ignorância dos consumidores, para usar tecnologia sob a justificativa de melhoria da experiência de compra dos consumidores, cuja existência, entretanto, eles sequer possuíam conhecimento, em detrimento de sua autonomia de vontade. (2020, p. 7)

Nesse sentido, a Senacon não enfrentou a questão de os dados serem anonimizados ou não, adotando como fundamento para justificar a violação a falta de transparência ao consumidor de que seus dados estariam sendo coletados (ainda que de forma anônima). É curioso que a Senacon faz menção à falta de consentimento dos consumidores, uma vez que, pela LGPD, o dado anonimizado não estaria sujeito às bases legais exigidas para a legitimidade do seu uso. E, sobre esse ponto, vale transcrever a forma como a Senacon evita o debate sobre a anonimização interferir na exigência (ou não) de consentimento:

> Outrossim, consta, em uma das manifestações da representada, argumento no sentido de que o fato de o consentimento dos consumidores não ser exigível na espécie não quer dizer que a representada não tenha adotado salvaguardas e mecanismos de proteção ao consumidor. Nesse ponto, a representada explica que os mecanismos que resguardam a esfera privada do consumidor estão incorporados no próprio bojo da tecnologia. É importante ressaltar, no entanto, que o referido argumento carece de qualquer comprovação nesse sentido. De qualquer forma, ainda que ficasse devidamente comprovada que os dados tenham sido comprovadamente captados e aplicados de forma anônima ou anonimizada, isso é despiciendo para a caracterização da infração ora apurada, uma vez que a ideia de dado anonimizado serve para afastar o conceito de dado pessoal – enquanto informação relacionada a pessoa natural identificada ou identificável – para fins de aplicação da LGPD (art. 12 da Lei 13.709/2018), que sequer se encontra em vigência no presente momento. (2020, p. 7)

Portanto, a Senacon descarta o debate técnico sobre anonimização e a consequente análise de necessidade de consentimento, optando por penalizar a Hering por violação aos direitos básicos do consumidor, em especial o direito de liberdade de escolha (art. 6º, II, do CDC), o direito de acesso à informação (art. 6º, III, do CDC) e o direito de proteção contra práticas abusivas em cláusulas contratuais (art. 6º, IV, do CDC). Sobre esse ponto, a "gramática" protetiva adotada pela Senacon se revela na medida em que o debate técnico sobre anonimização, o qual poderia ser utilizado pela empresa investigada para limitar a sua responsabilidade ou sustentar a legalidade da atividade de tratamento, não foi enfrentado.

5.3. Base legal

De acordo com a LGPD, "base legal" é a hipótese que autoriza o controlador a utilizar dados pessoais para uma finalidade determinada. Nela, estão previstas dez bases legais[82] para o

[82] "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I – mediante o fornecimento de consentimento pelo titular; II – para o cumprimento de obrigação legal ou regulatória pelo controlador; III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV – para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V – quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII – para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. (...)."

tratamento de dados pessoais não sensíveis (art. 7º da LGPD) e sete bases legais[83] para o tratamento de dados pessoais sensíveis[84] (art. 11 da LGPD).

Anteriormente à LGPD, as legislações esparsas que abordavam aspectos sobre o tratamento de dados pessoais baseavam-se quase que exclusivamente no consentimento do titular dos dados para autorizar o tratamento de dados pessoais. A Lei do Cadastro Positivo (Lei 12.414/2011), em sua versão anterior à Lei Complementar 166/2019, previa o consentimento como requisito para abertura de cadastro dos consumidores no sistema do cadastro positivo[85] (art. 4º da LCP). De forma semelhante, a Lei de Acesso à Informação (Lei 12.527/2011) também adotava como regra geral o consentimento expresso do titular de dados pessoais para o acesso a informações pessoais no âmbito da lei (art. 31, § 1º, II, da LAI), em que as demais situações previstas pela Lei de Acesso à Informação seriam uma exceção à exigência do consentimento do titular (art. 31, § 3º, I a V da LAI).

O Marco Civil da Internet (Lei 12.965/2014) também atribuiu centralidade ao consentimento enquanto hipótese autorizativa para o tratamento de dados pessoais. De acordo com o MCI, são direitos dos usuários da internet: a obtenção de "consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais" (art. 7º, IX), e o "não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei" (art. 7º, VII). Além disso, o MCI também veda a guarda de "dados pessoais que sejam excessivos em relação à finalidade para a qual

[83] "Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. (...)."

[84] Ver item 5.4, que trata sobre os conceitos de "Dado Pessoal" e "Dado Pessoal Sensível".

[85] Redação anterior à Lei Complementar 166/2019: "Art. 4º A abertura de cadastro requer autorização prévia do potencial cadastrado mediante consentimento informado por meio de assinatura em instrumento específico ou em cláusula apartada".

foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais" (art. 16, II).

Ao longo da década legislativa da LGPD, o consentimento foi perdendo gradualmente seu protagonismo no texto legislativo (BIONI, 2019, p. 133). Na primeira versão do Anteprojeto de lei colocado à consulta pública em 2010, o consentimento estava previsto como a única base legal para o tratamento de dados pessoais. Já na versão da segunda consulta pública de 2015, o consentimento era a regra geral para o tratamento de dados pessoais, sendo as demais hipóteses condições de dispensa do consentimento. Por fim, o texto enviado à sanção do Congresso Nacional já previa o consentimento como uma dentre nove hipóteses de tratamento igualmente aplicáveis para dados pessoais não sensíveis. No texto sancionado, a superioridade hierárquica do consentimento foi prevista apenas para o tratamento de dados pessoais sensíveis e dados de crianças.

A estratégia regulatória adotada pela LGPD de prever diversas bases legais igualmente aplicáveis para o tratamento de dados pessoais reflete padrões internacionais recentes da regulação da proteção de dados pessoais, especialmente do GDPR. O avanço da capacidade de processamento de dados e os ganhos sociais e de mercado decorrentes desse avanço justificaram a previsão de uma maior autonomia e flexibilidade para os agentes de tratamento de dados pessoais. Trata-se de prerrogativa especialmente relevante para os casos em que a obtenção do consentimento do titular do dado seria prejudicial para o atendimento de objetivos socialmente desejáveis, como o tratamento de dados para a proteção da vida ou integridade física do titular (como em situações de desastres, acidentes e catástrofes naturais), o atendimento de interesses legítimos (como o processamento de dados para a autenticação do titular dos dados e a prevenção à fraude), entre outras situações em que as finalidades de uso de dados pessoais seriam aceitáveis ante os seus benefícios para o próprio titular de dados pessoais ou para a sociedade como um todo.

Por outro lado, essa maior flexibilidade foi equilibrada por meio da previsão de mecanismos de prevenção a tratamentos "abusivos". Sobre esse ponto, a LGPD prevê "freios e contrapesos", por meio de princípios[86] (art. 6º da LGPD) e requerimentos legais direcionados aos agentes de

[86] "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II – adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV – livre acesso: garantia, aos titulares, de

tratamento. Por exemplo, a base legal do legítimo interesse, a mais ampla da LGPD para o tratamento de dados pessoais não sensíveis, tem um artigo dedicado exclusivamente a conferir salvaguardas na sua aplicação, conforme transcrito a seguir:

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
> I – apoio e promoção de atividades do controlador; e
> II – proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
> § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
> § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
> § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Com relação ao tratamento de dados sensíveis[87], a LGPD determina que o seu uso pode ocorrer "quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas" (art. 11, I) e as demais hipóteses autorizativas apenas podem basear o tratamento de dados pessoais sensíveis quando forem indispensáveis para as suas respectivas finalidades (art. 11, II), como a realização de estudo por órgão de pesquisa, a tutela da saúde em procedimentos realizados por profissionais da saúde, serviços de saúde ou autoridade sanitária, entre outras. Nesse sentido, na LGPD, o consentimento é a regra geral para o tratamento de dados pessoais sensíveis e as outras hipóteses autorizativas são exceções à regra geral do consentimento (dado o requisito de "indispensabilidade" para suas respectivas finalidades).

---

consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V – qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI – transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII – segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII – prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X – responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas."

[87] De acordo com a LGPD, dados sensíveis são aqueles sobre "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (art. 5º, II, da LGPD).

Com relação aos dados de crianças e adolescentes, a LGPD determina que "o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse" (art. 14, *caput*), devendo, em relação aos dados de crianças, "ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal" (art. 14, § 1º).

Na Senacon, das 33 notas técnicas analisadas, em 28 delas o conceito de base legal estava presente. Em todas essas 28 notas técnicas, a Senacon mencionava a necessidade do consentimento para autorização do tratamento de dados pessoais. Dentre as 28, 1 tangenciou a base legal do cumprimento de obrigação legal ou regulatória. Dentre as 5 notas técnicas que não trataram do tema da base legal, 4[88] tinham por objeto incidentes de segurança da informação e 1[89] tratava da mineração e comercialização de dados pessoais. O dado de que a maior parte das decisões que não envolveram o conceito de base legal diz respeito à incidentes de segurança da informação faz sentido porque, em incidentes, o "uso indevido de dados" ocorre independentemente da legalidade dos tratamentos anteriores (isto é, se os tratamentos de dados tinham "lastro" em uma base legal adequada), bastando o acesso não autorizado ou situações acidentais ou ilícitas de destruição, perda, alteração, compartilhamento ou exposição de dados em decorrência de uma falha ou vulnerabilidade de segurança.

Outro dado relevante é a centralidade do consentimento nas decisões tomadas pela Secretaria. Na entrevista realizada com o ex-servidor, uma possível justificativa para a centralidade do consentimento (e a justificativa para a sua centralidade) foi colocada da seguinte maneira:

> O consentimento é um ponto mais claro de como ligar a LGPD ao CDC, pelo direito à informação. Porque você vai pela linha do direito à informação, você chega no consentimento de uma forma muito clara. Então talvez por isso a SENACON tenha enfatizado tanto essa questão do consentimento.

O "consentimento" aplicado pela Senacon é semelhante ao previsto no Marco Civil da Internet. Inclusive, em algumas decisões, a Secretaria aplicou de forma expressa os dispositivos do MCI, no qual o consentimento deve ser expresso, livre e informado.

[88] Averiguação Preliminar Processo nº 08012.002376/2017-88 (C&A), Averiguação Preliminar Processo nº 08000.030856/2019-30 (Química Amparo), Averiguação Preliminar Processo nº 08012.000145/2018-11 (Netshoes) e Averiguação Preliminar Processo nº 08012.003074/2018-16 (Sky).
[89] Averiguação Preliminar Processo nº 08012.001400/2019-23 (J&A Holding).

A Senacon adotou o entendimento de que o consentimento deveria ser expresso na investigação em face do Google, sobre o escaneamento do conteúdo de e-mails[90]. Nesse caso, entendeu que a Política de Privacidade do Google, ao não prever de forma expressa a finalidade do escaneamento do conteúdo de e-mails, violou o dispositivo que determinava a obtenção de um consentimento expresso do usuário quanto à coleta, uso, armazenamento e tratamento de seus dados pessoais. Vale transcrever a linha de raciocínio da Secretaria para construir essa argumentação:

> Conforme se verifica no caso em comento, a Política de Privacidade do Google parece usar de expressões evasivas e que aparentemente não informam ao consumidor, com clareza, sobre a coleta e tratamento de dados, especialmente no que diz respeito ao Gmail. Apesar de acessível – i.e., não rebuscada – a linguagem usada pela empresa aparentemente não é capaz de plenamente fazer o consumidor entender as consequências de contratar os serviços da Google, o que vai de encontro à transparência e boa-fé necessárias para o equilíbrio das relações de consumo. (2019, p. 3)

Com relação ao consentimento ser livre, na decisão do caso *Cambridge Analytica*[91], a Secretaria adotou o entendimento de que a obtenção do consentimento por meio de uma caixa pré-selecionada por padrão prejudicaria a liberalidade/racionalidade da manifestação do titular de dados pessoais pelo uso de um mecanismo de *nudge*, conforme se verifica no trecho transcrito a seguir:

> Neste particular, o que se tem é que a Representada utilizou um *nudge* (um estímulo de comportamento) em que o compartilhamento instantâneo de informações de amigos de usuários que tenham aderido a um determinado aplicativo se dá num mecanismo *opt-out*, em vez de *opt-in*. Ainda, segundo Richard Thaler e Cass Sunstein, um *nudge* "é um estímulo, um empurrãozinho, um cutucão; é qualquer aspecto da arquitetura de escolhas capaz de mudar o comportamento das pessoas de forma previsível sem vetar qualquer opção e sem nenhuma mudança significativa em seus incentivos econômicos. Para ser considerada um *nudge*, a intervenção deve ser barata e fácil de evitar. Um *nudge* não é uma ordem. Colocar as frutas em posição bem visível é um exemplo de *nudge*. Simplesmente proibir a *junk food*, não. (THALER, Richard; SUNSTEIN, Cass. *Nudge*: O empurrão para a escolha certa. Trad. Marcello Lino. Rio de Janeiro: Elsevier, 2009, p. 8). (...) E é esse mecanismo que se encontra subjacente à dinâmica de um *nudge*: fazer com que pessoas tomem decisões que não seriam tomadas na ausência dos mesmos. Não há nada de ilícito nisso, obviamente. Utiliza-se tal mecanismo em várias instituições existentes no país, tais como regimes complementares de previdência (com adesão automática de servidores e fixação de um plano *default*, mas com possibilidade de desligamento e de alteração do plano de investimento contratado), no próprio Código de Defesa do Consumidor (ao tratar, nos arts. 103 e 104, dos efeitos da litispendência e da coisa julgada nas ações coletivas para a defesa de interesses individuais homogêneos), dentre outras.

[90] Averiguação Preliminar Processo nº 08012.004630/2015-11.
[91] Processo nº 08012.000723/2018-19 (averiguação preliminar); Processo nº 08012.000723/2018-19 (processo administrativo).

> Todavia, isso impõe uma maior responsabilidade ao aplicador do *nudge*. E não é à toa que os agentes decisores responsáveis pela gestão de fundos de pensão e de outros ativos se submetem a um escrutínio estrito tanto no Brasil como em vários lugares do mundo, seja em relação a acionistas minoritários, seja em relação aos participantes dos fundos, seja em relação a outros agentes e organizações que não tenham incentivos para uma participação relevante nesses processos decisórios.
> (...) Os Representados, pela adoção de um modelo de negócios que implicava em um padrão de configuração (decorrente de um *nudge*) de compartilhamento automático de dados de amigos (ou amigos de amigos etc.) de usuários com os aplicativos utilizados por esses últimos, deveriam ter um cuidado muito maior na gestão desses dados, uma vez que o modelo de consentimento adotado teve implicações relevantes para o número de pessoas com dados expostos (o qual é certamente muito maior do que se fosse adotado um modelo de *opt-in* para tal compartilhamento de tais dados). (2020, p. 14)

O requisito de liberdade do consentimento também apareceu no caso do Google sobre a coleta de dados de crianças e adolescentes no YouTube para o direcionamento de publicidade[92]. Nessa decisão, a Senacon indicou que Termos e Condições não seriam meios aptos para a coleta de um consentimento livre, dada a caracterização desse tipo de contrato como de adesão, em que não há possibilidade de negociação das cláusulas contratuais, conforme se verifica no trecho transcrito a seguir:

> Em que pese a afirmação do Representado de que o consumidor consentiria com a coleta de dados por estar prevista nos Termos de Serviço, é necessário ter cautela, tendo em vista que o consumidor não possui o poder de negociar tais cláusulas, assim como ocorre em um contrato de adesão. (2019, p. 4)

Com relação ao consentimento ser informado, a Senacon entendeu que, em algumas situações, o titular de dados pessoais não era suficientemente informado no momento de coleta do consentimento. No caso *Cambridge Analytica*[93], a Senacon discorreu longamente sobre a generalidade do consentimento coletado pelo Facebook por meio da sua Política de Privacidade, conforme se verifica a seguir:

> Ainda, é importante deixar claro que, o caráter "genérico" do consentimento obtido pela plataforma Facebook em face de seus usuários não pode ser visto como um "cheque em branco" para que esses dados sejam disponibilizados a quem quer que seja.
> (...) Isso colocado, ainda que haja inserção, nos termos de uso da plataforma, da possibilidade de compartilhamento instantâneo de dados de usuários discutida na presente nota, tal autorização de compartilhamento se deu em caráter genérico, uma vez que, *ex ante*, permaneciam em abertos dois pontos: a) que agentes concretamente teriam acesso a esses dados (notadamente, os desenvolvedores de aplicativo na plataforma) e b) qual a finalidade do tratamento das informações fornecidas pelos consumidores da plataforma. (2019, p. 21)

[92] Averiguação Preliminar Processo nº 08012.002781/2019-68.
[93] Processo nº 08012.000723/2018-19 (averiguação preliminar); Processo nº 08012.000723/2018-19 (processo administrativo).

Outro ponto tocado pela Senacon com relação ao consentimento foi a mudança da finalidade para a qual o consentimento teria sido obtido originalmente. Na decisão do processo administrativo do Cetelem[94], a Senacon entendeu que o uso de dados pessoais obtidos com o consentimento para uma finalidade distinta daquela informada na sua coleta constituiria violação da legislação consumerista:

> O uso de bases de dados de terceiros, nesse contexto, evidencia, portanto, uma grave violação à legislação consumerista não só pela ausência de comunicação prévia, mas também porque o uso desses dados para fins não consentidos pelo seu titular configura desvio de finalidade de sua coleta. (2021, p. 13)

A definição adotada na LGPD para o consentimento é de uma "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Ainda, em seu art. 8º, a LGPD dispõe sobre os requisitos e elementos necessários para a validade do consentimento do titular dos dados:

> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
> § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.
> § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.
> § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.
> § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.
> § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do *caput* do art. 18 desta Lei.
> § 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

Além disso, a LGPD estabelece que, para o compartilhamento de dados pessoais tratados com base no consentimento do titular de dados pessoais, é necessário consentimento específico do titular para o compartilhamento de dados pessoais com outros controladores, exceto quando possível a aplicação das outras bases legais previstas na legislação (art. 7, § 5º, da LGPD). E, em caso de mudança de finalidade de dados pessoais tratados com base no consentimento, o

[94] Processo Administrativo nº 08012.001476/2019-59.

controlador deve informar o titular de dados pessoais sobre as mudanças de finalidade, para que ele possa revogá-lo, caso discorde dessas mudanças (art. 9, § 2º, da LGPD).

Conforme se verifica nos trechos supratranscritos, em sua maioria, as qualificações colocadas pela Senacon sobre consentimento convergem com os dispositivos previstos na LGPD. Por exemplo, o consentimento ser uma manifestação livre, informada, e voltado a finalidades determinadas. Inclusive, a Senacon teve de decidir casos que teriam previsão legal na LGPD, sem equivalentes nas legislações anteriores. Por exemplo, sobre quando há mudança de finalidade do tratamento de dados.

Contudo, a principal diferença entre as decisões da Senacon analisadas no âmbito da pesquisa e o modelo regulatório adotado pela LGPD no que concerne a "bases legais" está na centralidade do consentimento para a legitimidade do tratamento de dados pessoais. Conforme mencionado anteriormente, ao longo do processo legislativo da LGPD aconteceu uma mudança de foco no tópico das bases legais, em que o consentimento perdeu sua centralidade para um arranjo legal que comporta outras hipóteses autorizativas do tratamento de dados pessoais. Nesse sentido, fossem as condutas investigadas pela Secretaria analisadas pelas lentes da LGPD, poderia ser imperioso enfrentar questões sobre o enquadramento da base legal ao caso concreto, em que as empresas investigadas poderiam argumentar pela legitimidade do tratamento com base em seu "legítimo interesse", para "execução do contrato" ou "proteção ao crédito", entre outras bases legais.

A Secretaria, em geral, não admitiu a possibilidade de as empresas investigadas se valerem de outras bases legais. Nesse sentido, o conceito de base legal se relaciona com a "gramática" protetiva da Senacon na medida em que a Secretaria adota uma base legal mais conservadora, que centra no consumidor a decisão de autorizar o uso de seus dados pessoais.

5.4. Dado pessoal

Caso a LGPD fosse um edifício, o conceito de dado pessoal estaria na sua fundação. Isso porque, em síntese, ela é aplicável ao tratamento de dados pessoais[95]. O conceito de tratamento é

[95] Em linhas gerais, a LGPD se aplica ao "tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado". De toda forma, vale pontuar que existem regras específicas quanto ao escopo territorial (art. 3º da LGPD), bem como de limitação material (art. 4º da LGPD) na aplicação da Lei.

bastante amplo na legislação, englobando "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (art. 5º, X, da LGPD). Nesse sentido, o conceito de dado pessoal é o núcleo determinante para o escopo de aplicação da lei.

De acordo com a LGPD, dado pessoal é a "informação relacionada a pessoa natural identificada ou identificável" (art. 5º, I). Dentro da categoria de dado pessoal existe a subcategoria específica de dado pessoal sensível, sendo este o "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (art. 5º, II). Dados os riscos relacionados à discriminação no uso de dados pessoais sensíveis, estes recebem, em alguns casos, requisitos adicionais para o seu tratamento, como a primazia do consentimento enquanto base legal[96].

Vale ressaltar que o CDC já previa uma seção dedicada aos bancos de dados e cadastros de consumidores (Seção VI, arts. 43-44). Na obra coletiva que reúne comentários dos autores do Anteprojeto do CDC (GRINOVER et al., 2007), Antônio Herman de Vasconcellos e Benjamin discorre sobre o contexto social e político que o levou a incluir no anteprojeto legislativo um dispositivo relacionado a dados e cadastro de consumidores.

Com o advento das "vendas a prazo", entre as décadas de 1950 e 1960, as decisões relacionadas à viabilidade do seu financiamento eram feitas com base no preenchimento minucioso de cadastros de dados pessoais dos consumidores, "não só com seus dados pessoais, mas indicando ainda os locais onde habitualmente adquiria produtos e serviços, como o armazém, a alfaiataria e, em especial, outros estabelecimentos onde já comprara a prazo" (p. 412). No princípio, tinha-se uma atuação individual dos comércios na compilação do histórico de crédito de seus consumidores. Ao longo do tempo, essa atividade evoluiu para um modelo empresarial coletivo de formação do histórico de crédito de consumidores, com o surgimento das associações civis de proteção ao crédito, o Serviço de Proteção ao Crédito (SPC).

[96] Ver tópico sobre "Base Legal" no item 5.3.

Entre a metade da década de 1950 e o início dos debates legislativos do CDC, essas associações, atualmente conhecidas como "*bureaus* de crédito", ganharam relevância cada vez maior. Nas palavras de Herman Benjamin:

> Decorrência do aparato tecnológico e humano dessas organizações é o fato de exercerem poder e influência igualmente impressionantes (para não dizer assustadores), mais ainda quando, sabe-se, operam elas em parceria, permutando informações entre si, mediante convênios que firmam. (2007, p. 413)

Além disso, o autor salientou que existiam também preocupações quanto aos riscos relacionados ao uso dessas informações e os impactos decorrentes para o consumidor:

> Eram notórios os abusos imputáveis a essa modalidade recente de coleta, organização e prestação de informações sobre a idoneidade pessoal e financeira das pessoas. Informações levadas ao conhecimento público, divulgadas pelos mais diversos meios de comunicação, em procedimentos banalizados, ensejando, como seria de se esperar, insatisfação generalizada, decorrência natural da gravidade e frequência de suas incursões indevidas. Foram esses fatos que me levaram a redigir a presente Seção (...). (BENJAMIN, 2007, p. 411)

Ainda, a Seção VI do CDC teria sido mais inspirada em iniciativas legislativas norte-americanas do que de direito comunitário europeu (à exceção de outros dispositivos do Código), como o *First Draft* do *National Consumer Act*, proposto pelo *National Consumer Law Center*, e o *Fair Credit Reporting Act* – a predecessora americana da Lei do Cadastro Positivo brasileira (BENJAMIN, 2007, p. 411).

Nos termos transcritos a seguir, o art. 43 da referida Seção do CDC articula os conceitos de "cadastro", "dados", "fichas", "registros" e "banco de dados" para conferir proteção aos consumidores em relação ao acesso, qualidade e uso de suas informações:

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
> § 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
> § 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
> § 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
> § 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
> § 5º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.

> § 6º Todas as informações de que trata o *caput* deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.

Os conceitos de "banco de dados" e "cadastro de consumidores" se relacionam com o conceito de "dado pessoal" da LGPD, ainda que os primeiros tenham surgido em um contexto histórico anterior para enfrentar um problema particular daquele momento em que a escala e a proeminência do processamento de dados pessoais eram muito menores do que atualmente. De acordo com Herman Benjamin, no CDC,

> (...) a *ratio* do codificador foi abarcar com as duas denominações [bancos de dados e cadastro de consumidores] todas as modalidades de armazenamento de informações sobre consumidores, sejam elas privadas ou públicas, de uso pessoal do fornecedor ou abertas a terceiros, informatizadas ou manuais, setoriais ou abrangentes. (2007, p. 432)

De forma semelhante, a LGPD adotou um conceito amplo para "dado pessoal", já que seu significado inclui todas as informações que possam identificar um indivíduo direta ou indiretamente (isto é, através do seu agrupamento/perfilamento).

No âmbito das investigações estudadas, a Senacon recorreu ao conceito de "banco de dados" do CDC, como na investigação do Facebook sobre o incidente na Amazon[97] em que entendeu que "os dados que são coletados dos consumidores em ambiente virtual formam os bancos de dados de caráter pessoal" (2019, p. 3). Para a Senacon, os bancos de caráter pessoal são constituídos por "informações (...) que trazem consigo aspectos intrinsicamente ligados à personalidade do indivíduo como: nome, sobrenome, endereços, opções religiosas, afetivas entre outras" (2019, p. 3).

Ainda que aparente adotar uma definição ampla para bancos de dados de caráter pessoal, em alguns casos, a Secretaria pareceu não incluir dentro do conceito os dados pessoais de identificação indireta, conforme se verifica no trecho transcrito a seguir:

> Os dados dos consumidores, de certo, requereriam proteção da Representada, especialmente aqueles ligados à personalidade, tais como: nome, sobrenome, endereços e outros. Além destas informações com caráter pessoal, outras também deveriam ser objeto de proteção, como curtidas, comentários, fotos, músicas, informações sobre amigos, eventos e até reservas de voos e hotéis. (2020, p. 4)

[97] Averiguação Preliminar Processo nº 08012.001086/2019-89.

Essa mesma definição mais restrita do conceito de informações com caráter pessoal também foi adotada pela Secretaria na investigação do vazamento de dados da Tim[98], conforme trecho a seguir:

> Como o Tim Negocia se trata de uma plataforma de negociação de dívidas, diversos dados dos consumidores requereriam proteção da Representada, especialmente aqueles ligados à personalidade, tais como: nome, sobrenome, endereços e outros. Além destas informações com caráter pessoal, outras também deveriam ser objeto de proteção, como o valor das dívidas cobradas, a forma de pagamento e dados relacionados. (2019, p. 2)

Nesse sentido, para a Senacon, ainda que fossem objeto de proteção, informações como "curtidas, comentários, fotos, músicas, informações sobre amigos, eventos e até reservas de voos e hotéis" (2020, p. 1), ou "valor das dívidas cobradas, a forma de pagamento e dados relacionados" (2019, p. 2) não estariam explicitamente dentro do conceito de "informação de caráter pessoal". Ainda que, ao final, a Secretaria entendesse que essas "outras" informações também seriam objeto de proteção, comparativamente, é possível identificar uma diferença conceitual entre as informações de caráter pessoal para a Secretaria e o conceito de dado pessoal da LGPD. Isso porque, para a LGPD, essas outras informações estariam inclusas no conceito de dado pessoal, já que o conceito expansionista da legislação inclui, além das informações diretamente relacionadas a pessoa natural, as informações relacionadas a pessoa natural que seja identificável (é o caso de informações comportamentais, como curtidas, comentários, viagens).

Outra diferença se refere ao conceito de dado sensível. Enquanto a LGPD prevê uma lista taxativa dos dados considerados sensíveis, a utilização do termo "sensível" pela Senacon foi menos precisa, usada em diversos contextos como uma característica das informações de caráter pessoal, isto é, toda a informação de caráter pessoal seria sensível, não havendo diferenciação pelo tipo de informação e seu potencial uso discriminatório. Por exemplo, no caso do incidente envolvendo uma plataforma da Tim, a Senacon, ao introduzir a investigação, qualifica o objeto da investigação da seguinte forma: "suposto vazamento de dados sensíveis e valores de dívidas dos consumidores por meio do TIM Negocia" (2019, p. 1).

No caso da Tim, vale ressaltar que a estratégia da empresa foi no sentido de alegar que os dados envolvidos no incidente não incluiriam dados pessoais sensíveis, alegação a que a Senacon rebateu da seguinte forma:

[98] Averiguação Preliminar Processo nº 08012.001392/2019-15.

> Além disso, com relação à alegação de que não houve exposição de dados pessoais sensíveis, não ficam afastados indícios de ocorrência de dano aos direitos de personalidade ao consumidor. Explica-se: o fato de haver tal exposição não impede que haja o tratamento desses dados para fins de *profiling* de consumidores (dentre outros propósitos), sem o consentimento e para as mais diversas finalidades (afinal de contas, ainda resta totalmente ignorado o destino a que os dados expostos foram submetidos). Fica o risco de possibilidade de triangulação de tais dados com outros dados pessoais sensíveis em outras bases. Assim, na melhor das hipóteses, permanece a exposição de dados pessoais sensíveis com a permanência do risco de utilização de tais dados até para a desanonimização de bases de dados que contenham dados pessoais sensíveis. (2019, p. 4)

Por outro lado, em duas investigações, a Secretaria pareceu adotar um conceito de "dado sensível" compatível com aquele previsto na LGPD. No caso do Facebook[99],

> (...) aplicativos que se encontram ligados no compartilhamento de informações com o Facebook podem estar cedendo, sem o consentimento dos consumidores, dados sensíveis, como: peso, pressão sanguínea, ciclo menstrual, status de gravidez, além de localização do usuário e visualização do valor de bens imóveis. (2019, p. 4)

Ainda que localização do usuário e valor de bens imóveis não estivessem dentro do conceito de dado pessoal sensível da LGPD, as informações relacionadas à saúde, como "peso, pressão sanguínea, ciclo menstrual e gravidez", estariam. No caso da Hering[100], a Senacon também caracterizou o dado biométrico, supostamente coletado por meio de tecnologia de reconhecimento facial, como dado sensível, de forma compatível com a definição de dado pessoal sensível da LGPD.

Conforme se verifica nos trechos supratranscritos, existe uma compatibilidade conceitual entre as definições de "dado pessoal" da LGPD e "informação de caráter pessoal" do CDC, especialmente dada a amplitude que ambos os conceitos comportam. Contudo, comparativamente, é possível dizer que a aplicação dos conceitos de "informação de caráter pessoal" e "dado sensível" pela Senacon tem um rigor conceitual menor do que aquele previsto pela LGPD, tendo em vista a não caracterização de informações diretamente relacionadas a consumidores como dado pessoal ou a acepção de que a sensibilidade de uma informação existiria em decorrência do seu caráter pessoal e da possibilidade de formação de perfis de consumidores. Trata-se de interpretação que se relaciona com a "gramática" protetiva da Secretaria, na medida em que adota um conceito amplo de informação de caráter pessoal e, por vezes, interpretação mais conservadora no sentido de

[99] Averiguação Preliminar Processo nº 08012.000520/2019-1.
[100] Averiguação Preliminar Processo nº 08012.001387/2019-11; Processo Administrativo nº 08012.001387/2019-11.

adjetivar como “sensível”, mesmo as informações não relacionadas ao rol taxativo de dados sensíveis previsto na LGPD.

5.5. Incidente de segurança da informação

A LGPD não traz uma definição para o conceito de “incidente de insegurança”. Todavia, ele pode ser extraído do *caput* do art. 46, que integra a seção sobre Segurança e Sigilo de Dados. Nesse artigo, a lei dispõe que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas para proteção dos dados pessoais contra situações de “acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito”.

Essa definição foi confirmada pela ANPD em fevereiro de 2021 na orientação sobre a comunicação de incidentes[101], em que ela define “incidente de segurança” como

> (...) qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

Com relação aos incidentes de segurança da informação, o ex-servidor da Senacon entrevistado nesta pesquisa relatou a dificuldade da Secretaria em realizar perícias nesse tipo de incidente, tendo em vista o alto nível de conhecimento técnico necessário para avaliação das causas e impacto da sua ocorrência. Foi no contexto dessas investigações que a Senacon recomendou a contratação de empresas independentes de auditoria, conforme detalhado no item 4.3.2, *supra*. Além disso, o entrevistado relatou ainda que, nesses casos, dada a dificuldade de comprovação do incidente, eram frequentes os arquivamentos: “A gente atuou também em alguns vazamentos de dados, acho que teve o da C&A se não me engano, mas muitos acabaram não sendo comprovados, então os processos acabam sendo arquivados (...)”.

Em relação ao enquadramento jurídico dos incidentes pela Senacon, interessante notar que a roupagem dada pela Secretaria no caso de um ataque *hacker* sofrido pelo Facebook teria sido de “vício na prestação do serviço”, conforme trecho a seguir:

[101] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Acesso em: 30 abr. 2022.

> Houve vazamento de dados decorrente da prestação de serviço com vício – pois não teria sido oferecida a segurança e a confiança que dele se poderia esperar – como aparenta ser o caso dos autos, em que hackers teriam invadido contas de usuários brasileiros cadastrados na plataforma Facebook, é necessário que se analise eventual responsabilidade das empresas pela reparação do dano, objetivamente, nos moldes do art. 18 do CDC. (...) Conclui-se, dessa forma, que, aparentemente, houve falha na prestação do serviço dos fornecedores Facebook Inc. e Facebook Serviços online do Brasil, o que teria permitido que terceiros pudessem utilizar indevidamente dados sensíveis dos consumidores. Isso se constitui em risco da atividade desenvolvida pelos Reclamados de aglutinarem em massa informações dos usuários e serem responsáveis pela segurança dessas informações, de modo que possam vir a ser responsabilizados diretamente pelos danos causados. (2019, p. 4)

Essa ideia de vício na prestação do serviço é uma visão baseada no fundamento normativo da proteção do consumidor. No mundo corporativo, é corrente a ideia de que incidentes devem ser encarados como um risco iminente, mesmo quando há a adoção dos melhores padrões e *frameworks* de segurança da informação. Isso porque mesmo os sistemas mais seguros podem ter sua vulnerabilidade explorada por pessoas com conhecimento técnico avançado em sistemas de informação ou em engenharia social[102]. Diversas empresas do setor de tecnologia, cientes de que os riscos técnicos dificilmente são anulados, têm desenvolvido programas conhecidos como *Bug Bounty*, em que oferecem recompensas a indivíduos que relatam *bugs* (erros) em suas plataformas e sistemas, em especial de vulnerabilidades relacionadas à segurança, para que atualizações possam ser feitas e vulnerabilidades, corrigidas, de forma a prevenir a exploração destas por terceiros[103].

Com relação aos incidentes analisados no âmbito da pesquisa, quatro envolveram *hackers* (também referenciados como "invasores" ou "cibercriminosos" nas notas técnicas) e um envolveu um pesquisador da área de segurança. Foram os casos da Netshoes[104], Facebook[105], Tim[106], Química Amparo[107] e Sky[108].

No caso da Netshoes, a empresa teria recebido um e-mail de um terceiro remetente não identificado afirmando "que possuía inúmeros dados de clientes, e que os divulgaria caso não ocorresse o pagamento de 1000 (mil) Bitcoins a determinada carteira virtual" (2019, p. 1). No caso

[102] No contexto da segurança da informação, ataques de engenharia social envolvem a exploração de uma vulnerabilidade do ser humano para a obtenção de acesso a informações confidenciais.
[103] A título de exemplo, ver o da Apple (https://support.apple.com/en-in/HT201220) e o da Intel (https://www.intel.com/content/www/us/en/security-center/default.html). Acesso em: 1º maio 2022.
[104] Averiguação Preliminar Processo nº 08012.000145/2018-11.
[105] Averiguação Preliminar Processo nº 08012.002467/2018-02.
[106] Averiguação Preliminar Processo nº 08012.001392/2019-15.
[107] Averiguação Preliminar Processo nº 08000.030856/2019-30.
[108] Averiguação Preliminar Processo nº 08012.003074/2018-16.

do Facebook, a empresa, "ao perceber anomalias no tráfego de usuários da plataforma, decorrente de pico nas métricas desses tráfegos, verificou que a irregularidade se tratava de atividade maliciosa realizada por terceiros invasores" (2019, p. 2). No caso da Tim, uma plataforma da empresa teria sido "objeto de ação criminosa" (2019, p. 2). No caso da Química Amparo, foram identificados

> (...) acessos considerados anormais ao portal 'Promoção Ypê' ao que sugere a análise, abusando dos mecanismos de autenticação para acessar dados de outros participantes do portal, seja de forma manual e aleatória, seja de forma sequencial ou ainda ao se utilizar de ferramentas para identificar eventuais vulnerabilidades do referido. (2020, p. 2).

Vale ressaltar que, no caso da Tim, a responsabilidade da empresa não foi afastada em decorrência da ação de cibercriminosos:

> Primeiramente, cumpre destacar que o fato de a exposição de dados ter se dado mediante a ação de cibecriminosos não elide a responsabilidade objetiva nos termos do art. 14 do CDC, podendo somente se eximir (art. 14 § 3º) quando demonstrar que, tendo prestado o serviço, o defeito inexiste e quando houver culpa exclusiva consumidor ou de terceiros. (2019, p. 4)

Por fim, no caso da Sky, um pesquisador de segurança independente identificou um "erro de configuração em um servidor *ElasticSearch* da AWS" e o comunicou ao *site* TecMundo, que publicou a notícia. De acordo com a Sky, a empresa teria corrigido a vulnerabilidade "30 minutos após o contato do site Tecmundo, tempo esse que permitiu a exposição temporária de arquivos de logs armazenados no servidor que continha dados pessoais dos consumidores da Representada".

Um ponto interessante a ser comentado sobre essa questão da responsabilidade é que, por vezes, terceiros utilizam bases de dados vazadas anteriormente para realizar ataques a outros sistemas. Nesse sentido, pode ser que um terceiro, que obteve as credenciais de acesso vazadas de um dado usuário de uma plataforma X, faça uso essas mesmas credenciais para tentar acessar as plataformas A, B e C. Nos casos em que usuários adotam as mesmas credenciais de acesso em diversas plataformas, essa vulnerabilidade se intensifica, ao passo que o vazamento de uma delas pode permitir que terceiros tenham acesso às demais aplicações que o usuário tenha utilizado mesmo login/senha são utilizados.

No sistema da LGPD, quando há a ocorrência de um incidente de segurança que possa acarretar risco para os direitos e liberdades do titular dos dados pessoais, o controlador deve comunicar a ANPD, descrevendo a natureza dos dados pessoais afetados, os titulares de dados pessoais envolvidos, as medidas técnicas e de segurança adotadas para a proteção dos dados, os

riscos gerados pelo incidente, as medidas que foram ou serão tomadas para reversão ou mitigação dos efeitos prejudiciais do incidente, entre outras informações (art. 48, I a VI, da LGPD).

Nas decisões sobre incidente de segurança da Senacon, não foi possível identificar um padrão de critérios adotado pela Secretaria para avaliação dos incidentes ou das obrigações a que os investigados estariam sujeitos quando da ciência do incidente. Os critérios em geral variavam de acordo com o caso e a postura do investigado em relação à análise e reparação dos danos causados pelo incidente. Em algumas situações, a Senacon avaliou parte dos elementos anteriormente citados, como as informações que foram prestadas aos titulares envolvidos, as medidas técnicas que foram adotadas para mitigação dos danos relacionados ao incidente e a proatividade do investigado na resposta ao incidente.

Com relação às informações prestadas aos titulares envolvidos no incidente, esse elemento apareceu no caso da Química Amparo, no trecho a seguir:

> Além disso, [a Química Amparo] registra que criou o Portal da Transparência, já mencionado alhures, site contendo todos os detalhes a respeito do incidente, a explicação das medidas adotadas e recomendações aos consumidores. Ainda, por meio de seu Serviço de Atendimento ao Consumidor (SAC), colocou-se à disposição para sanar quaisquer dúvidas dos consumidores. Salienta que, passados mais de dez meses da detecção do ilícito, a interessada "recebeu o contato de apenas 9 (nove) contatos, de 8 (oito) consumidores". (2020, p. 3)

Com relação às medidas técnicas adotadas na resposta do incidente, vale ressaltar os planos de resposta aos incidentes da C&A[109], da Netshoes e da Sky. No caso da C&A, as medidas envolveram questões técnicas de segurança de sistemas, como medidas administrativas de governança corporativa, conforme se verifica no trecho transcrito a seguir:

> De todo modo, implementou as seguintes medidas a fim de promover a segurança do sistema e dos clientes: (i) Aumento da restrição no uso das contas de e-mail coletivas utilizadas nas Lojas C&A (doc. nº 1), com o bloqueio do acesso externo dessas contas (docs. nºs 2 e 3), e restrição dos destinatários permitidos para o envio de e-mails (doc. nº 4); (ii) Revisão das regras de servidor para bloqueio da rede das Lojas C&A a sites de caixa de e-mails externos, sites de envio de informações em massa, WhatsApp web e site do SERASA (doc. nº 5); (iii) Extinção dos procedimentos de envio de dados por meio de ferramentas não criptografadas e encerramento do procedimento denominado de Saque Controle (doc. nº 6); (iv) Realização, em outubro de 2017, de campanha interna intitulada "Mobilização ética" visando reforçar aos funcionários, associados e lideranças da C&A os termos do Código de Ética, cultura e valores da empresa, assim como enfatizar os cuidados com dados fornecidos por clientes (doc. nº 7); (v) Início, em dezembro de 2017, de estudos quanto à viabilidade de implementação de aplicativo de comunicação online interna – do tipo *instant messenger* – que permitia maior governança pela empresa no

[109] Averiguação Preliminar Processo nº 08012.002376/2017-88.

> compartilhamento de dados; (vi) Contratação de empresa de consultoria visando o mapeamento, a partir de maio de 2018, de todo o processo de concessão e atendimento do cartão C&A; (vii) Contratação de empresa de consultoria especializada em Gestão de Acessos para implementar, em julho de 2018, nova ferramenta de gestão de acessos que aumentará a governança do processo e aprimorará a rastreabilidade dos acessos em diversas aplicações utilizadas pela C&A. A ferramenta de gestão será parametrizada com perfis de acesso, os quais serão revistos até fevereiro de 2019; (viii) Inclusão, em janeiro de 2018, de inquirição no programa de auditoria visando apurar se as Lojas C&A estão seguindo adequadamente as orientações quanto à proibição de uso de telefone celular em áreas críticas, tais como promotorias e caixas; e (ix) Contratação de empresa de consultoria especializada em Segurança da Informação visando implementar serviços de monitoramento contínuo da infraestrutura tecnológica, com o uso de ferramentas voltadas à identificação e solução de eventuais incidentes de segurança da informação, tais como tentativas de vazamento de dados e correlacionamento de logs de acessos a aplicações e ferramentas críticas. (2020, p. 3)

O plano de resposta a incidentes da Netshoes foi menos técnico e mais genérico, incluindo a revisão de processos corporativos, a qualificação do pessoal, entre outras medidas, conforme se verifica no trecho transcrito a seguir:

> A Representada também teria se comprometido a: "1) implantar medidas adicionais ao seu Programa de Proteção de Dados, quais sejam: gerenciamento de riscos e vulnerabilidades no portal Netshoes; ações de adequação à Lei Geral de Proteção dos Dados Pessoais; e atualização contínua de sua Política de Segurança Cibernética; 2) realizar esforços de orientação de consumidores, a aumentar o nível de conhecimento sobre os riscos cibernéticos e medidas de proteção de seus dados pessoais, por meio de campanha de conscientização; e 3) disseminar ao mercado as melhores práticas para privacidade e proteção de dados pessoais, por meio da participação em fóruns e eventos especializados; e difusão de boas práticas de proteção dos dados. (2019, p. 2)

O plano de resposta a incidentes da Sky foi o mais completo, incluindo tanto uma análise detalhada do incidente, quanto medidas técnicas de correção da vulnerabilidade. Além disso, a empresa também se comprometeu com mudanças corporativas de governança, adotando um *framework* baseado em princípios para a proteção dos dados, conforme se verifica no trecho transcrito a seguir:

> Em relação às medidas adotadas, a Representada apresentou que logo da correção do problema, com suporte de auditores externos da PwC, iniciou um processo de revisão de todos os seus sistemas para assegurar que não continham erros de configurações similares. Além do mais, adotou medidas preventivas e ações para evitar ameaças cibernéticas, dentre elas: "a. Análise interna de doze contas AWS; b. Alteração de senhas e logins; c. Revisão das regras de segurança da SKY; d. Revisão e aperfeiçoamento dos controles de acesso; e. Alteração do endereço de IP; f. Alteração das chaves – gateway API; g. Alteração do URL Load Balancer; h. Remoção de publicação dos sites; i. Fechamento de todos os 700 Buckets".
> Com relação às contas AWS, foram tomadas as seguintes medidas: "a. Alteração do caminho API Digital: API/IID do consumidor/login-CPF; b. Configuração do Setup e WAF em API Digital; c. Remoção de 70 tabelas Dynamodb referentes à AWS em São Paulo; d. Remoção de 55 tabelas Dynamodb referentes à AWS em Virgínia; e. Remoção

> de 12 buckets S3 (armazenamento da AWS)". Por fim, realizou-se também: "a. Avaliação e análise de eventuais vulnerabilidades da API mobile.sky.com.br (API do antigo aplicativo da SKY, anterior ao Minha SKY); b. Análise de antigos códigos API, que estavam desativados em razão da inatividade das fontes".
> No que tange aos instrumentos dispostos a efetivar a proteção de dados dos usuários, a Representada comunicou que desenvolveu e implementou uma política corporativa de "Proteção às Informações da Empresa e à Privacidade Individual", a qual tinha por objetivo definir todos os controles necessários à proteção da confidencialidade e integridade dos dados pessoais de seus clientes e funcionários, sendo assim, as seguintes medidas foram adotadas:
> "Autenticação: todos os acessos a informações pessoais requeriam autenticação para confirmação da identidade do usuário.
> Autorização: todos os acessos a informações pessoais dependiam da demonstração da efetiva necessidade, e apenas eram concebidos após a devida autorização (gerência etc.). Níveis de necessidade e autorização eram implementados em cada um dos sistemas internos da SKY por meio de um sistema de identificação e gestão de acesso.
> Finalidade: todos os acessos a informações deveriam ser limitados ao propósito de sua solicitação; (i) era concedido acesso ao mínimo de informações necessário e pelo menor período de tempo possível, somente para atender aos propósitos da solicitação; e (ii) somente era concedido acesso a destinatários que efetivamente necessitavam de tais informações.
> Divulgação a terceiros: a divulgação ou uso de Informações da Empresa por terceiros dependia da formalização de um Termo de Confidencialidade ou de qualquer outro documento ou compromisso de confidencialidade aprovado pelo departamento legal. Adicionalmente, todos os terceiros que eventualmente obtivessem acesso a informações pessoais da SKY deveriam antes ser submetidos a um processo de "análise de risco de terceiros". Por meio desse processo, o time de segurança da SKY devia assegurar que que os devidos controles fossem implementados pelos terceiros para proteger os dados pessoais em poder da SKY.
> Comunicação e Treinamento: a SKY comunicaria essa política a todos os usuários de informações da Empresa. Adicionalmente, a Empresa forneceria o devido treinamento aos usuários para execução dessa política.
> Retenção e Destruição: os registros relativos a requisições de acesso, aprovações e indeferimentos (e cancelamentos) do direito de uso de Informações da Empresa seriam mantidos, de acordo com cada tipo de informação e com a natureza de seu uso. As Informações da Empresa seriam destruídas com métodos seguros, e em conformidade os registros empresariais e período de retenção, de acordo com cada tipo de informação."
> Outrossim, a Representada anexou duas tabelas relativas a medidas gerais de proteção e a medidas técnicas de proteção. (2020, p. 3-4)

Algo que chama atenção em todas as medidas de mitigação adotadas pelas empresas anteriormente citadas é que, além das medidas técnicas pontuais de reparação da vulnerabilidade que levou ao incidente, essas empresas adotaram também medidas estruturais voltadas à melhoria da governança da privacidade dentro de seus ambientes corporativos, com o estabelecimento de políticas internas, a promoção de treinamentos de conscientização, a adoção de processos internos de avaliação e gestão de riscos, entre outras.

A responsividade e a proatividade de parte das investigadas na resposta aos procedimentos administrativos (e aos incidentes de segurança) levaram ao arquivamento de investigações na Secretaria, como foi o caso da Sky, que foi encerrado nos seguintes termos: "sugere-se o

arquivamento do presente feito por exaurimento de finalidade, em razão da já tomada de medidas por parte da Sky" (2020, p. 5).

Nesse contexto, é interessante notar que o arquivamento decorre de uma proatividade da empresa investigada na análise e adoção de medidas de mitigação dos danos ocasionados pelo incidente. Isso porque, ainda que medidas reparatórias tenham sido tomadas, dados ainda teriam sido expostos e/ou armazenados de forma não segura. Na LGPD, existe a previsão de que a adoção de medidas técnicas adequadas à proteção de dados pessoais deveria ser considerada para a avaliação da gravidade do incidente (art. 48, § 3º, da LGPD).

Ne entrevista, o ex-servidor da Secretaria relatou que a Senacon não teria uma definição clara sobre essa questão, mas que a sua percepção seria de que a Secretaria tenderia a favorecer empresas responsivas e diligentes:

> O que eu vejo nas autoridades é que todas têm consciência do quão difícil é proteger uma base de dados por mais forte que seja a segurança. Então quando uma empresa chega na Secretaria com uma atitude de colaboração, isso é muito bem-visto. E uma coisa que ainda não está bem definida lá dentro, e aí eu acho que, de novo, a gestão vai acabar impactando, é saber se as sanções vão ser aplicadas. Teve um vazamento que foi resolvido, se vai ter sanção ou, se por ter sido resolvido, se não vai ter sanção.

Ante o exposto, é possível afirmar que os casos investigados na Senacon como "incidente", "vazamento" e "exposição" de dados de consumidores poderiam ser considerados, sob a perspectiva da LGPD, como incidentes de segurança. Além disso, vale ressaltar que diversos dos elementos analisados pela Secretaria, ainda que de forma não padronizada, repetiriam aqueles previstos como de comunicação obrigatória à ANPD. Nesse sentido, com relação aos incidentes de segurança, parece haver relativa aproximação entre as notas técnicas analisadas da Senacon e o paradigma regulatório da ANPD[110].

5.6. Titular

A LGPD define o titular como a "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento" (art. 5º, V). Nesse sentido, a LGPD adota uma categoria ampla e universal para o titular dos dados pessoais, incluindo qualquer pessoa cujos dados pessoais tenham sido objeto de tratamento no território nacional; cujos dados tenham sido tratados para a oferta ou

[110] Ver item 5.8 para os incidentes relacionados a tratamentos considerados inadequados ou ilícitos.

fornecimento de bens ou serviços para pessoas localizadas em território nacional; ou que tenham sido coletados de indivíduos localizados em território nacional (art. 3º, I a III, da LGPD). O titular de dados é o sujeito de direito a quem a LGPD confere prerrogativas e direitos com o objetivo de garantir e instrumentalizar alguns de seus fundamentos, como o respeito à privacidade e o exercício da autodeterminação informativa.

Vale ressaltar que, por se tratar de um desdobramento dos direitos de personalidade, a titularidade dos dados pessoais[111] não está na ordem das relações patrimoniais – de posse ou propriedade –, sendo uma garantia de toda pessoa natural, conexa aos demais direitos e garantias fundamentais[112] (art. 17 da LGPD). Ainda, seguindo padrões internacionais de proteção de dados, a LGPD traz direitos específicos que oferecem instrumentos de controle para o titular sobre os seus dados pessoais, conforme dispõem os arts. 18 e 20 da Lei, transcritos a seguir:

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> I – confirmação da existência de tratamento;
> II – acesso aos dados;
> III – correção de dados incompletos, inexatos ou desatualizados;
> IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V – portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
> VI – eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII – informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII – informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX – revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.
> (...)
> § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.
> (...)
> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

[111] "Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei."
[112] A Emenda Constitucional 115/2022 acrescentou ao rol de direitos fundamentais (art. 5º da CF/88) o inciso LXXIX, segundo o qual "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".

Os direitos previstos na LGPD têm por intuito garantir a autodeterminação informativa, permitindo que titulares de dados pessoais possam ter autonomia sobre como suas informações são utilizadas. Ainda que seja uma proteção ampla conferida aos titulares de dados, algumas críticas são feitas ao atual modelo. Essas críticas incluem (i) a assimetria de poder entre titulares de dados e agentes de tratamento de dados; (ii) a ideia de que o acesso à informação não resulta, necessariamente, em escolhas mais conscientes dos titulares de dados; e (iii) a ideia de que uma categoria universal e individualizante de titular de dados não é apta a proteger grupos que podem ser mais severamente impactados pelo tratamento de dados, seja pelas suas condições sociais, políticas ou econômicas.

Com relação ao primeiro ponto, vale ressaltar que são poucas as empresas que permitem que os titulares de dados pessoais configurem para quais finalidades desejam que seus dados sejam tratados, por exemplo, por meio de painéis de privacidade[113]. Em geral, a política de tratamento de dados pessoais para o acesso a serviços, aplicativos e produtos é fornecida no formato de adesão com configurações por padrão, sem flexibilidade ou possibilidade de limitação da coleta ou finalidades do uso de dados pessoais, conforme trecho transcrito na decisão sobre publicidade infantil em face do Google[114]:

> Em que pese a afirmação do Representado de que o consumidor consentiria com a coleta de dados por estar prevista nos Termos de Serviço, é necessário ter cautela, tendo em vista que o consumidor não possui o poder de negociar tais cláusulas, assim como ocorre em um contrato de adesão. (2019, p. 4)

Shoshana Zuboff (2018, p. 48-49), ao discorrer sobre a assimetria de poder entre titulares de dados e agentes de tratamento, aponta para a forma que termos de uso de plataformas digitais são elaborados. O formato de adesão, com a aceitação por meio de um clique, muitas vezes faz com que as pessoas aceitem termos sem sequer ler as disposições contratuais. Soma-se a isso o fato de esses contratos serem longos, complexos e, por vezes, aplicáveis pelo simples fato de se acessar um determinado *website*. Além disso, não é raro que esses instrumentos possam ser atualizados de forma unilateral pelas empresas, sem a ciência ou anuência dos titulares de dados, sendo esse o modelo que rege a maior parte dos serviços e plataformas digitais.

[113] Um exemplo de Painel de Privacidade é o da Google, que permite a configuração granular sobre a coleta de dados como localização, histórico de navegação na web e vídeos assistidos no YouTube. Disponível em: https://myaccount.google.com/data-and-personalization?pli=1. Acesso em: 9 maio 2022.
[114] Processo nº 08012.002781/2019-68.

Além dos contratos de adesão, vale ressaltar que a limitação de parte dos direitos previstos no art. 18 da LGPD reforça essa assimetria. Por exemplo, o direito de anonimização, bloqueio ou eliminação de dados pessoais é limitado aos dados desnecessários, excessivos ou tratados em desconformidade com a legislação (art. 18, IV, da LGPD). No mesmo sentido, o direito de eliminação de dados pessoais é restrito aos dados pessoais tratados com base no consentimento do titular (art. 18, VI, da LGPD). Nesse sentido, não existe uma hipótese expressa na lei em que o titular de dados efetivamente poderia solicitar a um agente de tratamento a eliminação de seus dados pessoais, tendo os agentes de tratamento espaço para argumentar pela sua manutenção. Além disso, vale ainda ressaltar que o dispositivo que dispõe sobre a obrigação de descarte de dados pessoais prevê uma exceção para a obrigação de eliminação quando os dados foram sujeitos à transferência a terceiros (art. 16, III, da LGPD), o que, em uma cadeia complexa e ramificada de tratamento de dados pessoais, abre margem para a manutenção de dados pessoais de maneira indeterminada.

Com relação ao segundo ponto, sobre o acesso à informação não resultar em escolhas dos titulares que sejam mais protetivas de sua privacidade, existe na literatura um fenômeno denominado "paradoxo da privacidade". Essa expressão é associada à constatação de que, embora pesquisas de opinião mostrem que a privacidade *on-line* é uma questão importante para os indivíduos, as pessoas geralmente não protegem ativamente os seus dados pessoais e muitas vezes os divulgam voluntariamente em plataformas digitais (GERBER; GERBER; VOLKAMER, 2018).

Uma das possíveis explicações para o fenômeno é o fato de o acesso à informação dos titulares ser imperfeito. Ao aderirem aos termos e condições de uma determinada plataforma *on-line*, os titulares podem não compreender como seus dados pessoais serão usados por esses provedores de serviços, seja pelo ponto trazido anteriormente, de que as informações fornecidas sobre o processamento de dados pessoais não são claras, ostensivas ou acessíveis, seja pela falta de interesse do usuário em dedicar tempo para analisar tais informações.

Ainda, existe uma limitação de racionalidade dos titulares, que impossibilita que os titulares tenham ciência de todas as atividades de tratamento às quais seus dados pessoais estão sendo submetidos para poderem exercer um controle efetivo sobre os seus dados. Nesse sentido, na obra coletiva *Group Privacy* (2017), autores associam essa limitação de racionalidade com uma crítica ao modelo individual de exercício de direitos.

De acordo com os autores, o atual paradigma de proteção de dados foca no controle individual dos titulares sobre seus dados pessoais. Tanto a ideia de consentimento como requisito para o tratamento de dados pessoais de regimes de origem anglo-saxã, quanto os direitos de proteção de dados previstos pelos ordenamentos da Europa continental teriam a mesma falha de não reconhecer a dificuldade de o indivíduo ter noção ou controle sobre o tratamento de seus dados pessoais em uma realidade de *big data*, de cruzamento e processamento de grandes bancos de dados, entre outras práticas recorrentes. Essa falta de noção limitaria, inclusive, a possibilidade de o titular exercer seus direitos de oposição perante controladores de dados, ou de peticionamento perante autoridades (TAYLOR; VAN DER SLOOT; FLORIDI, 2017).

Com relação ao terceiro ponto, a crítica sobre a adoção de uma categoria universal de titular de dados adota como premissa a ideia de que os titulares de dados não são um grupo homogêneo de pessoas, igualmente impactados pelo tratamento de seus dados pessoais. Nesse sentido, essa concepção universalizante desconsidera o fato de que a privacidade pode ter significados e efeitos distintos para diferentes subgrupos, especialmente para pessoas que fazem parte de grupos historicamente marginalizados.

Sobre esse ponto, no painel "*Connecting the dots: privacy, data, racial justice*", organizado pela *London School of Economics*, parte do evento internacional *Computers, Privacy e Data Protection* (CPDP), Yasmine Boudiaf (2021) fez a seguinte reflexão[115]:

> Although data protection is usually cited as the key to controlling the power of big technology firms, its underlying premise which is the rational informed and liberal subject is vulnerable with respect to the new paradigms of big data and I would say that this is a criticism that's true not just of the GDPR but also about of much of our digital rights, which is, for the most part, centered on how we can just be better, more "savvy" users of technology and therefore use our legal tools to challenge this. I think this assumption is fundamentally based on a norm of the white middle class educated cis-het male who might have the resources and the knowledge to use their data protection rights to challenge some of these issues in many ways, but this framework does not meet the standards to be able to challenge the injustices that are experienced by peoples who do not meet that norm…

Tendo isso em mente, uma representação universalista de titulares de dados pode ser insuficiente para abordar efeitos e impactos interseccionais decorrentes do tratamento de dados pessoais, como pessoas negras, indígenas, mulheres, migrantes, analfabetas, LGBTQIA+, entre outras. Isso porque o tratamento de dados pessoais dessas pessoas pode ter impactos mais

[115] A captação do painel está disponível no YouTube: https://www.youtube.com/watch?v=Kfd_8pTBbXs. Acesso em: 9 maio 2022.

profundos em sua privacidade ou aumentar os efeitos discriminatórios no seu acesso ao mercado de trabalho, de consumo, de assistência social, entre outros.

Os pontos colocados acima se relacionam com a concepção de "titular de dados" adotada pela Senacon nas decisões analisadas, e a Secretaria, em especial, parece adotar um pressuposto normativo distinto daquele previsto na LGPD. Primeiro, vale esclarecer que a Secretaria não adota o conceito de "titulares de dados", tendo optado por mobilizar principalmente o conceito de "consumidores"[116]. Ainda que "consumidores" também seja uma categoria universalizante, o pressuposto normativo da vulnerabilidade do consumidor faz com que a aplicação do Direito pela Secretaria enfrente, em parte, as críticas anteriormente elencadas.

Nas decisões analisadas, a vulnerabilidade do consumidor foi central para a interpretação dos casos. Inclusive, a Secretaria declarou em mais de uma nota técnica que "não há como tratar de dados pessoais no âmbito das relações de consumo sem considerar a vulnerabilidade do consumidor" (2019, p. 3 – Tim; 2019, p. 3 – Hering; 2019, p. 3 – Facebook; 2019, p. 2 – Facebook; 2019, p. 6 – Google). Nas notas técnicas, o fundamento da vulnerabilidade do consumidor decorre do CDC (art. 4º, I), conforme trechos transcritos a seguir:

> Da leitura do art. 4º do CDC, percebe-se que há preocupação do sistema jurídico brasileiro em não causar desequilíbrios injustificados nas relações de consumo. Além disso, o CDC parte do pressuposto de que o consumidor é sujeito vulnerável ao adquirir produtos e serviços ou, simplesmente, ao se expor às práticas do mercado. (2019, p. 3)

> O Código de Defesa do Consumidor (CDC) prevê princípios que estabelecem as relações de consumo, dentre os quais um dos mais importante é o da vulnerabilidade do consumidor. Todos os demais princípios e direitos proveem do seu reconhecimento. A vulnerabilidade é percebida claramente diante da sua desigualdade fática no âmbito da relação entre consumidor e fornecedor. Nesse sentido, é necessária a ação governamental para coibir e reprimir de maneira eficiente todos os abusos praticados no mercado de consumo (art. 4º, *caput*, do CDC). (2019, p. 3)

> Nota-se que, entre os objetivos da Política Nacional das Relações de Consumo estão o respeito à dignidade, o atendimento à saúde e à segurança dos consumidores, a proteção dos interesses econômicos e a transparência e harmonia nas relações de consumo através do reconhecimento do princípio da vulnerabilidade.
> Nesse sentido, para Valério Dal Pai Moraes: Vulnerabilidade, sob o enfoque jurídico, é, então, o princípio pelo qual o sistema jurídico positivado brasileiro reconhece a qualidade ou condição daquele(s) sujeito(s) mais fraco(s) na relação de consumo, tendo em vista a possibilidade de que venha(m) a ser ofendido(s) ou feridos, na sua incolumidade física ou

[116] Interessante notar que a caracterização de usuários de plataformas como "consumidores" é fundamentada em precedentes do Superior Tribunal de Justiça: "Tais dispositivos se aplicam aos usuários de redes sociais, como o YouTube, por serem considerados consumidores apesar da aparente gratuidade na relação existente, segundo posicionamento do Superior Tribunal de Justiça (RESP n. 1316921RJ)" (2019, p. 3).

> psíquica, bem como no âmbito econômico, por parte do(s) sujeito(s) mais potente(s) da mesma relação. (2019, p. 4)

Em paralelo ao fundamento jurídico, a vulnerabilidade do consumidor também é justificada pela Secretaria por aspectos relacionados à caracterização do titular de dados, tanto de forma geral, quanto especificamente a grupos vulneráveis. No âmbito geral, a Secretaria associou a vulnerabilidade do consumidor com a limitação de racionalidade dos titulares de dados pessoais. No caso *Cambridge Analytica*[117], a Secretaria colocou que "há vasta literatura e evidências no sentido de que consumidores, em geral, tem dificuldades em dimensionar adequadamente as consequências futuras de decisões presentes, tomadas no momento da adesão aos termos de uso da plataforma" (2019, p. 15).

Sobre esse ponto, a Secretaria mobilizou a referência doutrinária de Bruno Bioni (2018, p. 144-147), transcrita a seguir:

> Dada a racionalidade limitada do ser humano, é pouco provável que ele esteja capacitado para tanto. Com efeito, a *bounded rationality* prescreve justamente que as habilidades cognitivas do ser humano são limitadas, minando a sua capacidade de absorver, memorizar e processar todas as informações relevantes para um processo de tomada de decisão. Já se faz impossível memorizar os inúmeros atores que compõem a referenciada rede social de publicidade, quanto mais compreender como os dados pessoais serão por eles tratados, já que cada um deles tem as suas respectivas políticas de privacidade. Soma-se, ainda, o complicador da compreensão de como a agregação dos dados pessoais desenrolar-se-á a ponto de extrair informações mais detalhadas sobre seus titulares. A complementar tal quadro problemático, há barreiras psicológicas que mistificam por completo a capacidade de o indivíduo controlar as suas informações pessoais. A primeira delas é a chamada teoria da decisão da utilidade subjetiva. O ser humano tem a tendência de focar nos benefícios imediatos, o que, de acordo com o arranjo e os modelos de negócios da economia informacional, é representado pelo acesso a um produto ou serviço on-line se de sopesar os possíveis prejuízos à privacidade, que são temporariamente distantes. De fato, os possíveis danos com relação à perda do controle sobre as informações pessoais só podem ser experimentados no futuro (...).

A ideia de racionalidade imperfeita também foi suscitada pela Secretaria no caso sobre o vazamento da Tim[118], em que a Senacon entendeu que a falta de conhecimento e capacidade técnica dos consumidores para a prevenção da vazamentos[119] dos seus dados pessoais também constituiria uma vulnerabilidade:

> No caso em comento, nota-se que pode ter ocorrido a violação da confiança do consumidor, tendo em vista que existiria uma brecha na plataforma Tim Negocia, que permitia que cibercriminosos acompanhassem dados pessoais e valores de dívidas de

[117] Processo Administrativo nº 08012.000723/2018-19.
[118] Processo Administrativo nº 08012.001392/2019-15.
[119] Ver item 5.5 – Incidentes de segurança.

> consumidor. Assim, em inobservância à vulnerabilidade do consumidor, que não possui a capacidade técnica de ter conhecimento e de se proteger contra tais violações especialmente em ambiente virtual. Assim, com a exposição de dados pessoais e relacionados a dívidas, os consumidores também foram expostos a possíveis práticas abusivas, tendo em vista que os dados poderiam ser utilizados de forma equivocada por terceiros não autorizados. (2019, p. 4)

E, sobre a vulnerabilidade do consumidor perante uma racionalidade imperfeita, vale ressaltar que esse argumento foi utilizado pela Senacon para justificar a intervenção estatal. Assim, mesmo no caso em que informações claras e completas foram aparentemente fornecidas para os consumidores, poderia haver abuso ou exploração de sua vulnerabilidade, conforme excerto a seguir:

> Qualquer mau uso, por um desenvolvedor, dos dados dos usuários da plataforma, terá consequências relevantes para a coletividade de seus consumidores, restando entendido, aqui, que o fornecimento de informações claras e completas (o que será objeto de avaliação em momento posterior) não se mostra suficiente para o adequado tratamento do problema ora narrado, demandando, em caráter excepcional, a intervenção estatal para a seu enfrentamento de forma menos imperfeita que a adoção, pura e simples, do modelo da escolha racional. Entre as duas alternativas (isto é, entre preservar uma falha de mercado ou correr o risco de se criar uma falha de governança, que trazem benefícios e vieses que lhes são próprios), fica-se com o risco da segunda. (...). (2019, p. 19)

Além do aspecto geral relacionado à racionalidade imperfeita de consumidores, vale notar que a Senacon também identificou contextos de maior vulnerabilidade para grupos específicos de titulares de dados, especificamente crianças, adolescentes e idosos.

Na averiguação preliminar em face do Google sobre a coleta de dados de crianças e adolescentes no YouTube para o direcionamento de publicidade, a Senacon dispõe que "tanto o Código de Defesa do Consumidor quanto a Constituição Federal e o Estatuto da Criança e do Adolescente colocam a criança sob seu abrigo, protegendo-a dos abusos publicitários e de situações em que sua integridade física ou psíquica esteja em perigo". E que a "utilização dos dados de menores, sem o conhecimento e consentimento deles ou dos responsáveis, para fins publicitários" representaria indícios de "violação ao inciso IV do artigo 39 do CDC, que veda que o fornecedor se prevaleça da fraqueza ou ignorância do consumidor, em razão de sua idade, para que possa impingir-lhe seus produtos ou serviços" (2019, p. 5).

Sobre esse tema, vale ressaltar que a LGPD também protege de forma específica crianças e adolescentes (art. 14 da LGPD). A lei exige que o tratamento de dados de crianças e adolescentes seja realizado em seu "melhor interesse" (art. 14, *caput*, da LGPD), sendo necessário o

consentimento[120] de um dos pais ou responsável legal para o tratamento de dados pessoais de crianças (art. 14, § 1º, da LGPD). Além disso, os mecanismos de transparência (como políticas ou avisos de privacidade) devem ser adaptados às "características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário"[121] (art. 14, § 6º, da LGPD).

A categoria de idosos foi mobilizada pela Senacon nas decisões envolvendo o uso de dados de idosos para telemarketing de empréstimo consignado por instituições financeiras. Para a Senacon, idosos apresentam uma condição de "hipervulnerabilidade", que é central para a constatação de prática abusiva, conforme trecho a seguir:

> Vale destacar que a presente averiguação envolve uma qualidade especial de consumidores: os idosos. Eles merecem atenção especial quanto à sua proteção, em razão da sua condição de hipervulnerabilidade na contratação dos empréstimos consignados e a sua propensão a se tornar um consumidor superendividado. Ademais, é importante destacar que esses consumidores merecem, ainda, uma proteção mais especial no âmbito da economia digital, pois normalmente encontram dificuldades adicionais para utilizar bens e serviços oferecidos em meio eletrônico, se comparados com o resto da população. Dessa forma, a hipervulnerabilidade do consumidor idoso é condição central, a qual exige análise mais apurada quando da aplicação do Código de Defesa do Consumidor nas relações de consumo, servindo como critério balizador de interpretação das normas e protegendo essa espécie de consumidor das práticas abusivas perpetradas em seu desfavor. (2021, p. 10)

Com relação à categoria de idosos, ela foi inserida na LGPD quando da conversão da MP 869/2018 em lei. Com essa alteração, a LGPD passou a dispor que à ANPD compete "garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento" (art. 55-J, XIX, da LGPD). Na Resolução CD/ANPD 2/22, que regula a aplicação da LGPD para agentes de tratamento de pequeno porte, a ANPD determina que a utilização de dados pessoais de idosos deve ser considerada um critério específico para o enquadramento de determinada atividade de tratamento como de alto risco (art. 4º, II, *d*, da Resolução CD/ANPD 2/22).

Ante o exposto, ainda que a Senacon adote a categoria universalizante de "consumidores", o pressuposto normativo da vulnerabilidade do consumidor faz com que, nas decisões analisadas, a Secretaria enderece algumas das críticas feitas às representações universais de titulares de dados adotadas pelas legislações gerais de proteção de dados, como é o caso da LGPD. Essa é uma

[120] Ver item 5.3 – Base legal.

[121] Esse foi o entendimento da Senacon no caso do Google envolvendo publicidade infantil, conforme trecho transcrito a seguir: "Ademais, é preciso adequar os termos de uso ao tratamento de dados do público de crianças e adolescentes, tendo em vista que possuem proteção jurídica diferenciada" (2019, p. 5).

abordagem que se relaciona diretamente com a "gramática" protetiva da Senacon, porque adota como premissa central a ideia de proteção dos consumidores ante a sua vulnerabilidade.

Com relação à vulnerabilidade, a Senacon reconhece tanto uma vulnerabilidade geral a todos os consumidores, caracterizada pela assimetria de poder e pela limitação da racionalidade do consumidor no momento da contratação, quanto grupos vulneráveis (como crianças, adolescentes e idosos). Isso não quer dizer que a LGPD não reconheça a vulnerabilidade do titular dos dados pessoais ou proteja grupos vulneráveis. Vale ressaltar que esse tipo de aplicação do Direito ainda pode vir a ser feito pela ANPD ou pelo Judiciário quando da interpretação da LGPD. O objetivo deste tópico foi mais explorar como o princípio da vulnerabilidade do consumidor, central nas decisões da Senacon estudadas, se relaciona com o conceito de "titular de dados" da LGPD.

5.7. Transparência

Na LGPD, a transparência está prevista como um princípio[122], uma obrigação dos controladores de dados pessoais[123] e um direito dos titulares de dados[124]. Enquanto obrigação imposta aos controladores, a LGPD estabelece o dever de transparência ativa, de informar. Enquanto princípio (garantia individual) e direito dos titulares, a LGPD estabelece um dever de transparência passiva do controlador, isto é, por meio da previsão aos titulares de um direito de obter acesso às informações referentes ao tratamento de seus dados pessoais.

[122] LGPD: "Art. 6º (...) VI – transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial" e "Art. 6º (...) IV – livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais".

[123] Por exemplo: "Art. 9º (...) § 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca" e "Art. 10 (...) § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse".

[124] Por exemplo: "Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso (...)" e "Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I – confirmação da existência de tratamento; II – acesso aos dados; (...) VII – informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII – informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa (...)".

Transparência e acesso à informação não são novidade para o regime do CDC, que garante aos consumidores o direito básico de ter acesso à "informação adequada e clara sobre os diferentes produtos e serviços" (art. 6º, III, do CDC), e o "acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes" (art. 43, *caput*, do CDC). Além disso, a transparência é um dos objetivos da Política Nacional das Relações de Consumo (art. 4º, *caput*, do CDC).

A LGPD, em seu art. 9º[125], estabelece quais seriam os requisitos necessários para a garantia de transparência sobre as atividades de tratamento de dados pessoais aos titulares de dados pessoais. Esse artigo orienta o conteúdo das Políticas de Privacidade, que tem por objetivo informar os titulares sobre como seus dados pessoais são informados. De acordo com o dispositivo, as informações devem ser disponibilizadas "de forma clara, adequada e ostensiva" e abranger a "finalidade específica do tratamento", a "forma e duração do tratamento", a "identificação do controlador", "informações acerca do uso compartilhado de dados pelo controlador e a finalidade", "direitos do titular", entre outras informações. Ainda, nas hipóteses em que o consentimento é a base legal do tratamento de dados, em caso de mudança de finalidade do tratamento de dados pessoais, há a obrigação do controlador de informar previamente o titular sobre as mudanças de finalidade, cabendo ao titular a possibilidade de revogar o consentimento anteriormente dado ao controlador.

Para a Senacon,

> (...) o direito à informação pressupõe que ela seja prestada de forma adequada, clara e inequívoca (quantidade, características, composição, qualidade, preço, riscos) sobre os diferentes produtos e serviços ofertados ao consumidor. A informação a ser prestada ao

[125] "Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I – finalidade específica do tratamento; II – forma e duração do tratamento, observados os segredos comercial e industrial; III – identificação do controlador; IV – informações de contato do controlador; V – informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI – responsabilidades dos agentes que realizarão o tratamento; e VII – direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei. § 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca. § 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações. § 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei."

> consumidor deve ser completa, gratuita e útil, de forma que o consumidor compreenda o que está adquirindo ou contratando. Ela é a essência do contrato e assegura a transparência na relação de consumo. (2020, p. 6)

Além de assegurar a transparência na relação de consumo, o acesso à informação é visto pela Secretaria como requisito essencial para a liberdade de escolha do consumidor, para que este possa exercer controle individual sobre suas informações, nos seguintes termos: "Nesse diapasão, a informação é essencial para que o consumidor tenha liberdade para escolher se deseja ou não compartilhar os seus dados com a finalidade de evitar práticas abusivas" (2019, p. 4).

Com relação a esse ponto, vale ressaltar que parte das investigações analisadas envolveu "Mecanismos de monitoramento ou vigilância" (conforme descrito no item 4.2.2, *supra*). Nessas situações, as decisões da Secretaria envolveram uma análise do cumprimento do dever de transparência pelas empresas investigadas. É interessante ressaltar que nesses casos em geral entendia-se que as informações sobre a finalidade de tratamento dos dados pessoais não eram claras, completas e, por vezes, sequer eram fornecidas.

Na investigação do Google sobre o *screening* de e-mails de usuários do Gmail[126], a Senacon entendeu que a linguagem utilizada pela empresa não era clara, tendo como consequência o fornecimento incompleto de informações ao consumidor, nos termos a seguir:

> Assim, também é fácil concluir que há indícios de informação incompleta ao consumidor, pelo teor da linguagem colocada. Quando se lê, na Política de Privacidade, por exemplo, que "Um cookie é um pequeno texto enviado ao seu navegador por um site que você visita. Ele ajuda o website a se lembrar de informações sobre a visita, como seu idioma preferido e outras configurações. Isso pode tornar sua próxima visita mais fácil e o site mais útil para você. Os cookies desempenham um papel importante. Sem eles, usar a Web seria uma experiência muito mais frustrante". Pode não ficar claro, para o consumidor, que o cookie é uma ferramenta que monitoramento de hábitos de usuários da Internet. O ordenamento jurídico e, frise-se, o direito do consumidor, especificamente, repudiam a conduta de informar apenas em parte ou de ocultar informação, seja por meio de atendentes seja por qualquer outra forma que conduza o consumidor a erro. (2019, p. 4)

Ainda, a Política de Privacidade sequer mencionava o escaneamento de e-mails, o que foi interpretado pela Secretaria como violação do Marco Civil da Internet:

> Com relação à possível violação às prescrições do Marco Civil da Internet, também podemos considerar que há indícios de não cumprimento do que está disposto no art. 7º, inciso IX dessa Lei, uma vez que o escaneamento dos e-mails não está, em nenhuma parte da política de privacidade, expresso ou destacado. (2019, p. 4)

[126] Processo nº 08012.004630/2015-11.

Outro caso envolvendo o monitoramento de consumidores foi a investigação da Hering, sobre o uso de tecnologia de reconhecimento/detecção facial de consumidores. No processo administrativo, a Senacon entendeu que o fato de a Hering não informar aos consumidores que eles estariam utilizando a referida tecnologia violaria o dever de informação, nos termos a seguir:

> Questionados por ocasião da reunião realizada (11325442), se os consumidores, ao entrarem na loja, sabiam, de alguma forma, que essa situação estava acontecendo em algum lugar, responderam que não houve um aviso específico sobre as câmeras, pois o fornecedor entendeu se tratar de questão simples, que não exigia comunicação específica sobre isso (...) É certo que a representada, ao realizar o uso de qualquer tipo de tecnologia para fim ora apresentado, deveria, ao menos, ter alertado adequadamente os consumidores, ainda que por um aviso inserido na entrada do estabelecimento, munindo-os com todas as informações, especialmente quanto à extensão da coleta e quanto à finalidade de aplicação dos dados coletados. (2020, p. 6)

Por fim, casos sobre transparência envolveram também questões relacionadas às práticas de compartilhamento de dados entre empresas. O Zoom foi investigado em decorrência de o seu código-fonte compartilhar automaticamente dados de usuários com o Facebook, mesmo daqueles usuários que não tivessem conta na plataforma, fato não previsto na Política de Privacidade, conforme o trecho a seguir:

> O que a empresa e sua política de privacidade não deixam claro é que a versão iOS do aplicativo Zoom está enviando alguns dados de análise para o Facebook, mesmo que os usuários do Zoom não tenham uma conta no Facebook, de acordo com uma análise do aplicativo na placa-mãe. (2020, p. 1)

No caso do incidente da Amazon, a Senacon entendeu que o Facebook não informava adequadamente os usuários sobre o armazenamento de informações por terceiros desenvolvedores de aplicativo: "No presente processo, o usuário/consumidor não tem o pleno acesso à informação da extensão da terceirização do uso da plataforma, de modo que é necessário analisar o direito à proteção digital do consumidor vulnerável ante a conduta das Representadas" (2020, p. 3).

E, no caso do Banco Pan, a Senacon entendeu que a instituição não deixava claro para os titulares as fontes dos números de telefone e dados cadastrais obtidos pelas correspondentes da instituição financeira, que eram utilizados para fins de telemarketing de consignado da instituição financeira (trecho a seguir). Vale ressaltar que, nesse caso, a Secretaria suspeitava que os dados tinham origem em um vazamento de uma base de dados do INSS, que era explorada por terceiros para direcionamento de publicidade a idosos e pensionistas da previdência.

"Ainda, o mesmo artigo prevê que os consumidores devem ter clareza sobre as fontes de informação que originaram o banco de dados" (2021, p. 7).

Nesse sentido, assim como na LGPD, a transparência foi tema relevante para a Senacon nos casos analisados. De acordo com a Secretaria, "o direito à informação pressupõe que ela seja prestada de forma adequada, clara e inequívoca" (2020, p. 6), devendo ser "completa, gratuita e útil" (2020, p. 6). A inexistência ou incompletude das informações sobre a "extensão da coleta e quanto à finalidade de aplicação dos dados coletados" revela infração ao direito de informação dos consumidores.

5.8. Uso indevido de dados

Conforme mencionado anteriormente, o dispositivo que define o que seria considerado um tratamento de dados pessoais irregular pela LGPD – provavelmente o análogo ao uso indevido de dados pessoais da Senacon – teve o seu desenho bastante aberto na lei, adotando termos indeterminados, como: "deixar de observar a legislação", "não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes", e não considerar "resultado e riscos que dele razoavelmente se esperam", entre outras hipóteses, conforme transcrição a seguir:

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando **não fornecer a segurança que o titular dele pode esperar**, consideradas as circunstâncias relevantes, entre as quais:
> I – **o modo pelo qual é realizado**;
> II – **o resultado e os riscos que razoavelmente dele se esperam**;
> III – **as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado**.
> Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

É interessante notar que o art. 44 da LGPD, supratranscrito, parece reproduzir a estrutura do art. 14 do CDC, que versa sobre a responsabilidade do fornecedor de serviços pela reparação de danos ao consumidor ocasionados pela prestação dos serviços, conforme disposto a seguir:

> Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.
> § 1º O serviço é defeituoso quando **não fornece a segurança que o consumidor dele pode esperar**, levando-se em consideração as circunstâncias relevantes, entre as quais:

I – **o modo de seu fornecimento**;
II – **o resultado e os riscos que razoavelmente dele se esperam**;
III – **a época em que foi fornecido**. (...).

Conforme se pode notar, o art. 44 da LGPD (assim como faz o CDC em seu art. 14) confere uma centralidade à ideia de segurança do titular de dados pessoais para a identificação de tratamentos irregulares. Anteriormente, o tópico 5.5 – Incidente de segurança da informação – tratou dos incidentes de segurança da informação. Paralelamente, pela própria leitura do art. 46 da LGPD, é possível perceber que os incidentes de segurança não se limitam a incidentes de segurança da informação, dado que o *caput* do artigo inclui também "qualquer forma de tratamento inadequado ou ilícito" no conceito de incidentes.

Nesse sentido, didaticamente, é possível dividir "incidentes de segurança" em duas subcategorias conceituais: incidentes de segurança da informação ("acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação de dados pessoais") e incidentes de privacidade ("tratamentos inadequados ou ilícitos"). Essa é uma separação conceitual que não encontra referencial teórico na literatura especializada, mas é útil para articular essas duas categorias de incidente de naturezas distintas. Enquanto os incidentes de segurança da informação têm relação com aspectos técnicos de segurança (e sigilo) da informação, voltados à garantia da integridade, disponibilidade e sigilo dos dados, os incidentes de privacidade teriam um aspecto normativo relacionado com a legitimidade do contexto de uso dos dados pessoais, em especial quando o tratamento pode impactar direitos fundamentais e garantias individuais de seus titulares. Em 2019, Miriam Wimmer já apontava a necessidade de um deslocamento da disciplina jurídica da proteção de dados de uma abordagem exclusivamente técnica, centrada na ideia de segurança da informação (enquanto sigilo e proteção contra acessos não autorizados a determinadas informações), para uma abordagem jurídica, no campo dos direitos fundamentais, assumindo a segurança da informação um caráter instrumental (no prelo, p. 2).

Assim, é pertinente concluir que o conceito de incidentes da LGPD faça referência, além dos incidentes de segurança da informação, a incidentes denominados anteriormente de "incidente de privacidade". No âmbito dos casos analisados na Senacon, os itens 4.2.5 – Vazamento de dados pessoais – e 4.2.6 – Falhas de segurança da informação – descrevem casos que poderiam ser classificados como incidentes de segurança da informação. Já os itens 4.2.1 – Comercialização de dados pessoais –, 4.2.2 – Mecanismos de monitoramento ou vigilância – e 4.2.3 – Compartilhamento de dados pessoais, sem autorização ou ciência dos titulares dos dados pessoais

– poderiam ser caracterizados como incidentes de privacidade, dada a ilicitude da finalidade ou irregularidade da forma de tratamento dos dados pessoais, considerando o contexto e o impacto nos direitos dos titulares de dados pessoais.

A Senacon não adota a expressão "incidente" para os casos acima classificados como "incidente de privacidade", fazendo-o apenas para os casos classificados como "incidentes de segurança da informação", inclusive adotando expressões correlatas, como "exposição de dados" ou "vazamento de dados". Contudo, é interessante destacar que os casos investigados pela Senacon também envolveram incidentes relacionados a aspectos de legitimidade ao contexto de coleta e tratamento de dados pessoais, como no caso do *Cambridge Analytca*, em que o incidente não foi resultado de uma vulnerabilidade técnica da plataforma, mas de decisões de negócios e da falta de controle administrativo adequado de governança de dados pessoais do Facebook.

Nesse sentido, as condutas caracterizadas como potenciais "usos indevidos de dados" pela Secretaria, nos termos das descrições feitas pela própria Senacon nas notas técnicas, foram as seguintes:

Tabela 2 – As condutas caracterizadas como "uso indevido de dados"

Processo Administrativo	**Representada**	**Conduta**
08012.004630/2015-11 (Averiguação Preliminar)	Google	"Ausência de consentimento expresso, parte do usuário, para a análise do conteúdo de e-mails pessoais enviados através do Gmail."
08012.000723/2018-19 (Averiguação Preliminar)	Facebook	"Os usuários da plataforma Facebook teriam realizado um teste de personalidade, por intermédio de um aplicativo, e teriam concordado em ter seus dados coletados para fins acadêmicos. Contudo, aparentemente sem consentimento dos usuários, também teriam sido coletados dados de todos os amigos dos usuários que fizeram o teste. Desta forma, a *Cambridge Analytica* teria, sem autorização, adquirido esses dados e os utilizado para catalogar o perfil das pessoas e dirigir, de forma individualizada, materiais de campanha nas eleições norte-americanas."
08012.002467/2018-02 (Averiguação Preliminar) 08012.000723/2018-19 (Processo Administrativo)	Facebook	"Pela notícia, o Facebook enviou, no dia 17 de outubro de 2018, mensagens para os brasileiros que tiveram dados privados acessados por hackers no mês de setembro. O Facebook não teria informado quantos usuários do país tiveram os dados pessoais acessados pelos criminosos, mas confirmou que, no mundo todo, o número chegava a 30 milhões. A notícia ainda

		comunicava que, entre os dias 14 e 27 de setembro de 2018, outros 60 milhões tiveram suas chaves digitais invadidas. Em consequência, suas contas foram bloqueadas, não sendo possível precisar se essas pessoas tiveram os dados pessoais roubados.”
08012.001478/2019-48 (Averiguação Preliminar) 08012.001478/2019-48 (Processo Administrativo)	BMG	“Extrai-se das denúncias apresentadas que instituições financeiras, mediante vazamento de dados dos aposentados e pensionistas vinculados ao Instituto Nacional do Seguro Social – INSS, estão realizando abordagens telefônicas de forma abusiva para que consumidores idosos adquiram empréstimo ou cartão de crédito consignado. Há registro, ainda, de que mesmo antes de auferir o primeiro benefício, os idosos estão a receber diversos contatos telefônicos com oferta de produtos na modalidade consignada. Segundo a denúncia apresentada, referida prática está levando os idosos a situação de superendividamento.”
08012.001492/2019-41 (Averiguação Preliminar)	Caixa Econômica Federal	
08012.001486/2019-94 (Averiguação Preliminar) 08012.001486/2019-94 (Processo Administrativo)	Safra	
08012.001483/2019-51 (Averiguação Preliminar)	Banco Olé	
08012.001470/2019-81 (Averiguação Preliminar) 08012.001470/2019-81 (Processo Administrativo)	Itaú Consignado	
08012.001490/2019-52 (Averiguação Preliminar)	Banrisul	
08012.001462/2019-35 (Averiguação Preliminar) 08012.001462/2019-35 (Processo Administrativo)	Banco Pan	
08012.001476/2019-59 (Averiguação Preliminar) 08012.001476/2019-59 (Processo Administrativo)	Cetelem	
08012.001488/2019-83 (Averiguação Preliminar)	Bradesco Financiamentos	
08012.001489/2019-28 (Averiguação Preliminar)	Bradesco	
08012.001387/2019-11 (Averiguação Preliminar)	Hering	“(...) existem indícios de que a vulnerabilidade do consumidor, caracterizada principalmente pelo desconhecimento da coleta e da respectiva finalidade, teve a sua intimidade violada com a captura de dados pessoais sobre gênero, faixa etária e humor, ou

08012.001387/2019-11 (Processo Administrativo)		mesmo com o alegado reconhecimento facial, com a finalidade de melhorar a publicidade dos produtos da Representada no estabelecimento."
08012.001392/2019-15 (Averiguação Preliminar)	Tim	"(...) suposto vazamento de dados sensíveis e valores de dívidas dos consumidores por meio do serviço TIM Negocia (...)."
08012.000520/2019-11 (Averiguação Preliminar)	Facebook	"(...) apuração de aparentes irregularidades cometidas pelas empresas Facebook Inc. e Facebook Serviços Online do Brasil Ltda. acerca da utilização de dados sensíveis, como frequência cardíaca e ciclo menstrual, mensagens e e-mails privados, bem como localização do consumidor e visualização de bens imóveis, obtidos por meio de aplicativos."
08012.000145/2018-11 (Averiguação Preliminar)	Netshoes	"(...) suposta exposição de dados pessoais dos consumidores cadastrados no e-commerce Netshoes, em aparente violação ao Código de Defesa do Consumidor."
08012.002781/2019-68 (Averiguação Preliminar)	Google	"(...) coleta de dados de geolocalização de menores (crianças e adolescentes) usuários do aplicativo YouTube (como localização, aparelho usado e número de telefone), da referida empresa, sem o conhecimento dos pais, para fins de publicidade dirigida ao público infantil."
08012.001400/2019-23 (Averiguação Preliminar)	J&A	"(...) suposta comercialização de dados pessoais e sigilosos de consumidores."
08012.002376/2017-88 (Averiguação Preliminar)	C&A	"(...) suposta prática de comercialização de dados pessoais e sigilosos dos consumidores cadastrados na empresa C&A MODAS S.A."
08012.003074/2018-16 (Averiguação Preliminar)	Sky	"(...) exposição de dados de consumidores, tais como: nome completo, e-mail, senha de login do serviço, endereço de IP, métodos de pagamento, número de telefone e endereço residencial, o que teria atingido 32 milhões de consumidores brasileiros clientes da Representada e usuários da TV por assinatura."
08000.030856/2019-30 (Averiguação Preliminar)	Ypê	"(...) suposto 'vazamento de dados pessoais' de consumidores participantes de campanha promocional da empresa Ypê (...)."
08012.002596/2019-73 (Averiguação Preliminar)	Facebook	"(...) em razão de notícia (9441947) sobre o pagamento de terceirizados para escutarem e transcreverem áudios de usuários de seus serviços, tais como o Messenger. Segundo noticiado, 'os funcionários das empresas contratadas ouvem as conversas dos usuários do Facebook, mas não sabem por que o Facebook as quer transcritas'."
08012.002762/2019-31 (Averiguação Preliminar)	Mercedes-Benz	"(...) suposta utilização do e-call na Europa, de forma indevida, com a finalidade de rastrear consumidores inadimplentes."
08012.000760/2020-41 (Averiguação Preliminar)	Zoom	"De acordo com a notícia (11368176), 'O que a empresa e sua política de privacidade não deixam claro é que a versão iOS do aplicativo Zoom está enviando alguns dados de análise para o

		Facebook, mesmo que os usuários do Zoom não tenham uma conta no Facebook, de acordo com uma análise do aplicativo na placa-mãe'. Segundo a matéria, 'O aplicativo Zoom notifica o Facebook quando o usuário abre o aplicativo, detalhes sobre o dispositivo do usuário, como o modelo, o fuso horário e a cidade da qual eles estão se conectando, de qual operadora de telefone eles estão usando e um identificador de anunciante exclusivo criado pelo dispositivo do usuário que as empresas podem usar para direcionar um usuário com anúncios'."
08012.001086/2019-89 (Averiguação Preliminar)	Facebook	"(...) aparentes irregularidades cometidas pelo Facebook que deixou vulneráveis os dados de seus usuários/consumidores, de modo que ficassem expostos em servidores da Amazon, sem qualquer tipo de senha de proteção."

Fonte: autoria própria

Por fim, nas investigações estudadas, embora o art. 14 tenha sido mobilizado nas notas técnicas para responsabilização dos fornecedores, o principal conceito utilizado pela Secretaria para o enquadramento jurídico do uso indevido de dados foi "prática abusiva", que é um conceito jurídico extraído do CDC (Seção IV – Das Práticas Abusivas). De acordo com o art. 39 do CDC, ao fornecedor é vedado: "condicionar o fornecimento de produto ou de serviço ao fornecimento de outro produto ou serviço, bem como, sem justa causa, a limites quantitativos"; "recusar atendimento às demandas dos consumidores, na exata medida de suas disponibilidades de estoque, e, ainda, de conformidade com os usos e costumes"; entre outras práticas consideradas abusivas.

Nas investigações analisadas, a prática abusiva era principalmente caracterizada em decorrência de o fornecedor supostamente "prevalecer-se da fraqueza ou ignorância do consumidor, tendo em vista sua idade, saúde, conhecimento ou condição social, para impingir-lhe seus produtos ou serviços" (art. 39, IV, do CDC), ou veicular publicidade enganosa/abusiva, sendo ela a "publicidade discriminatória de qualquer natureza, a que incite à violência, explore o medo ou a superstição, se aproveite da deficiência de julgamento e experiência da criança, desrespeita valores ambientais, ou que seja capaz de induzir o consumidor a se comportar de forma prejudicial ou perigosa à sua saúde ou segurança" (art. 37, § 2º, do CDC) e a publicidade que, por omissão, deixa "de informar sobre dado essencial do produto ou serviço" (art. 37, § 3º, do CDC).

Nesse sentido, nas notas técnicas analisadas, o uso indevido de dados foi enquadrado como prática abusiva ao consumidor, mesmo nos casos em que ela não estivesse prevista no rol do art. 39, já que "para a caracterização da prática abusiva não é necessário que a conduta esteja

expressamente descrita no art. 39 do CDC, uma vez que o rol ali colocado é exemplificativo" (2019, p. 4), servindo os princípios jurídicos do CDC como "parâmetros para a interpretação de práticas abusivas" (2019, p. 2).

Concluindo, "tratamento irregular" e "uso indevido de dados" podem ser considerados análogos, tendo como denominador comum o objetivo central de garantir a segurança do titular de dados/consumidor. As condutas enquadradas pela Senacon como "uso indevido de dados" poderiam ser classificadas, pela LGPD, como incidentes de segurança da informação e incidentes de privacidade. A Senacon, contudo, não adota esse conceito, mobilizando, por sua vez, o conceito de prática abusiva para enquadramento das condutas consideradas como "uso indevido de dados".

CONCLUSÃO

O objetivo da pesquisa foi compreender como a Senacon mobilizou o Direito nas 33 notas técnicas públicas conclusivas de averiguações preliminares e processos administrativos envolvendo dados pessoais que tramitaram entre fevereiro de 2019 e julho de 2021. Em especial, identificar as "palavras-chave", isto é, os conceitos que traduzem a "gramática" adotada pelo órgão para interpretar e decidir casos relacionados à tutela de dados pessoais, com o intuito de compreender como a abordagem da Senacon à proteção de dados pessoais se relaciona com os conceitos, regras e pressupostos normativos advindos da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018).

Originalmente, o interesse de pesquisar a atuação da Senacon surgiu da curiosidade sobre o sentido da expressão "uso indevido de dados" adotada pelo órgão para classificar uma série de eventos distintos envolvendo dados pessoais nos casos investigados pelo DPDC[127]. Primeiro, porque não há na LGPD qualquer referência literal à expressão "uso indevido de dados". Segundo, porque, salvo raras exceções[128], o legislador não estabeleceu *a priori* no texto legal as hipóteses ou finalidades para as quais o uso de dados pessoais estaria vedado.

Tendo em vista que a Senacon integra o arranjo institucional de proteção de dados pessoais no Brasil, dada a competência de órgãos de defesa do consumidor receberem reclamações dos titulares de dados pessoais em relação aos direitos previstos na LGPD (art. 18, § 8º, da LGPD), é relevante compreender como a Secretaria tem aplicado o Direito nos casos de "uso indevido de dados".

Logo na etapa exploratória da pesquisa, um elemento que chamou atenção foi a abordagem adotada pela Secretaria. Embora adotasse conceitos análogos ao previstos na LGPD, a Secretaria

[127] Essas investigações estão sendo amplamente divulgadas pela mídia. Ver: https://valor.globo.com/brasil/noticia/2020/09/24/uso-de-empresas-de-fechada-para-venda-ilegal-de-dados-entra-na-mira-do-governo.ghtml; https://noticias.r7.com/economia/ofertas-nem-sempre-sao-fidedignas-alerta-senacon-sobre-black-friday-27112020; e https://tecnoblog.net/405877/senacon-e-procon-sp-notificam-serasa-sobre-vazamento-de-220-milhoes-de-cpfs/. Acesso em: 17 fev. 2021.

[128] Algumas dessas exceções são: (i) o uso compartilhado de dados de saúde com o objetivo de obter vantagem econômica (art. 11, § 4º, da LGPD); (ii) o tratamento de dados de saúde por operadoras de planos privados de assistência à saúde para a prática de "seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários" (art. 11, § 5º, da LGPD); e (iii) o tratamento por pessoa jurídica de direito privado para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigações e repressões de infrações penais (art. 4º, § 2º, da LGPD).

parecia partir de pressupostos normativos distintos da LGPD. Essa percepção se desdobrou na questão central da pesquisa, que pode ser colocada da seguinte forma: como os conceitos que traduzem a abordagem da Senacon nos procedimentos administrativos analisados no escopo da pesquisa se relacionam com o paradigma conceitual-normativo da LGPD?

A conclusão foi no sentido de que, embora exista sobreposição e utilização de conceitos análogos aos da LGPD pela Senacon, a principal diferença entre a abordagem da Secretaria e o paradigma normativo da LGPD, que se fundamenta na autodeterminação informativa do titular de dados pessoais, com garantias individuais de controle, se dá de forma mais proeminente na adoção pela Senacon do pressuposto normativo da vulnerabilidade do consumidor como lente interpretativa nas decisões sobre os "usos indevidos de dados". O reconhecimento da vulnerabilidade do consumidor como elemento central de análise fez com que a atuação da Secretaria fosse orientada à sua proteção, prescindindo de um enfrentamento de questões técnico-normativas que poderiam ser suscitadas caso as condutas fossem interpretadas pela ótica da LGPD. Essa abordagem protetiva ao consumidor diante de sua vulnerabilidade em decorrência do uso de seus dados pessoais é o que caracteriza a "gramática" adotada pela Secretaria nos casos estudados.

A Nota Técnica nº 04/19[129], emitida durante a tramitação do projeto de conversão em lei da MP 869/2018, citada na introdução deste trabalho, evidenciara uma preocupação daqueles que então integravam a Secretaria, de que a nova configuração institucional da ANPD fosse "de encontro com os interesses dos consumidores", principalmente por conta da previsão de a Autoridade ser a última instância de interpretação da LGPD[130], nos seguintes termos:

> A nova competência preponderante da ANPD pode colocar em risco o andamento e *enforcement* dos processos administrativos em andamento – sem prejuízo de outros que possam porventura serem instaurados –, motivo pelo qual não faz sentido que a SENACON seja privada de atuar no âmbito de uma matéria que é inerente às suas competências. Mais do que isso, o consumidor brasileiro está num estágio menos avançado em relação à importância e ao valor econômico de sua privacidade e de seus dados se comparado aos consumidores europeus, tornando a aplicação do Código de Defesa do Consumidor (CDC) desejável nesse estágio de nosso desenvolvimento sócio cultural. (2019, p. 1)

[129] Nota Técnica nº 04/19/GAB-SENACON/SENACON/MJ, Processo nº 08012.001058/2019-61.

[130] Essa atribuição estava prevista na MP 869/2018 e foi confirmada quando da conversão da MP em lei, que é o seguinte dispositivo: "Art. 55-K. A aplicação das sanções previstas nesta Lei **compete exclusivamente à ANPD**, e suas **competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas** de outras entidades ou órgãos da administração pública. Parágrafo único. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e **será o órgão central de interpretação desta Lei** e do estabelecimento de normas e diretrizes para a sua implementação".

Conforme se verifica nessa declaração, o posicionamento daqueles que compunham o corpo técnico da Secretaria naquele momento adotava como premissa a ideia de que o consumidor brasileiro estaria "num estágio menos avançado em relação à importância e ao valor econômico de sua privacidade e de seus dados se comparado aos consumidores europeus". Essa narrativa seria utilizada na declaração para justificar a aplicação do CDC em casos envolvendo a tutela de dados pessoais, por ser o regime mais adequado ao "estágio de nosso desenvolvimento sociocultural". Em outras palavras, dado o estágio de desenvolvimento sociocultural brasileiro, a aplicação do CDC pela Secretaria em questões relacionadas à proteção de dados pessoais no âmbito das relações de consumo seria preferível.

Contudo, a nota técnica em referência não explicita quais seriam os dispositivos ou pressupostos normativos da LGPD ou da competência preponderante da (então futura) ANPD que poderiam ser prejudiciais ou incompatíveis com a proteção do consumidor, tendo em vista o "estágio menos avançado [dos consumidores brasileiros] em relação à importância e ao valor econômico de sua privacidade e de seus dados se comparado aos consumidores europeus".

Para decifrar tais pressupostos, vale ressaltar que a menção aos "consumidores europeus" na nota técnica faz referência ao fato de a LGPD ter sido, em grande medida, inspirada no Regulamento Geral de Proteção de Dados Europeu (RGPD) (UE) 2016/679. Conforme classificação de Viktor Mayer-Schönberger (1997) sobre as diferentes gerações de leis de proteção de dados europeias, a regulação na Europa sobre o tema evoluiu historicamente, desde a década de 1970, no sentido de garantir aos indivíduos a responsabilidade pela tutela de suas informações pessoais, buscando conferir ao titular de dados instrumentos que permitissem o exercício de sua autodeterminação informativa. Ocorre que, na nota técnica mencionada, a Secretaria adota como premissa a ideia de que os consumidores brasileiros não estariam aptos a reconhecer a importância e o valor econômico de sua privacidade e de seus dados pessoais, condição essencial para o exercício da autodeterminação informativa prevista nas legislações europeias (e na LGPD).

Conforme explorado no conceito de "titular de dados", não existe na LGPD um dispositivo que reconheça de forma expressa a vulnerabilidade do titular de dados ou permita a sua proteção *prima facie* em relação aos agentes de tratamento. Essa vulnerabilidade está presente de forma indireta na forma como a LGPD dedica critérios específicos para o tratamento de dados de crianças e adolescentes, regula as hipóteses de tratamento de dados sensíveis, bem como coloca freios e

contrapesos para o tratamento de dados pessoais, levando em consideração o respeito por direitos fundamentais, bem como os riscos e impactos decorrentes de seu uso. De toda forma, não há na LGPD dispositivo análogo ao do CDC que adote como pressuposto normativo a primazia da proteção do titular de dados pessoais ante objetivos concorrentes como desenvolvimento econômico e tecnológico ou a livre-iniciativa, como há atualmente no arranjo brasileiro de proteção do consumidor.

Nesse sentido, a premissa de que a aplicação do CDC seria preferível pode estar associada à centralidade de proteção do consumidor, decorrente do reconhecimento de sua vulnerabilidade no mercado de consumo. Essa centralidade da vulnerabilidade do consumidor pode, em parte, explicar o motivo de a Secretaria, por vezes, prescindir de uma análise técnica aprofundada sobre as condutas classificadas como uso indevido de dados e optar por decisões principiológicas baseadas em direitos básicos do consumidor (como os direitos de acesso à informação, de proteção do consumidor, de vedação à prática abusiva, entre outros). O reconhecimento da vulnerabilidade do consumidor, nesse contexto, seria uma regra para a Senacon, que permitiu a ela prescindir de questões técnico-normativas que estariam presentes nos casos investigados se fossem interpretados a partir do paradigma da LGPD. É, portanto, uma gramática em prol da defesa do consumidor ante os riscos relacionados ao tratamento de dados.

Essa abordagem ficou mais evidente nos conceitos de "agentes de tratamento", "anonimização", "base legal" e "titulares". Vale ressaltar que, embora a abordagem da Senacon aparente divergir do paradigma da LGPD em relação à caracterização dos titulares de dados como vulneráveis, é preciso pontuar que os direitos básicos previstos pelo CDC (como transparência, liberdade de escolha, entre outros) encontram correspondência na LGPD. Por exemplo, a falta de transparência poderia também ser considerada uma violação aos direitos dos titulares de dados pessoais, tendo em vista que a transparência é um princípio que norteia a aplicação da norma (art. 6º, I e VI, da LGPD), bem como um direito dos titulares de dados pessoais (art. 9º da LGPD). Nesse sentido, é possível que, no âmbito da supervisão e aplicação da LGPD, a ANPD adote pressuposto análogo ao da vulnerabilidade do consumidor. Também é possível que uma interpretação da LGPD nesse sentido tenha permeabilidade no Poder Judiciário. Até o presente momento, não existem dados que possam sustentar quaisquer dessas hipóteses, restando espaço apenas no campo da elucubração. De toda forma, vale reiterar que o reconhecimento da vulnerabilidade dos titulares de

dados pessoais em determinadas circunstâncias não anula a garantia da autodeterminação informativa, podendo, na realidade, atuar de forma complementar.

Todavia, ressalta-se que não é trivial o achado da pesquisa no sentido de identificar aquilo que caracteriza a "gramática" adotada pela Senacon nas notas técnicas estudadas. Primeiro, porque a Secretaria faz parte do arranjo de proteção de dados pessoais brasileiro. Segundo, porque a Senacon, por meio da sua atuação, pode influenciar a forma como outros atores interpretam e aplicam o Direito em casos envolvendo dados pessoais. E, por fim, porque a "gramática" adotada pela Secretaria, fundamentada no paradigma da proteção do consumidor ante o reconhecimento de sua vulnerabilidade em face dos agentes de tratamento, pode ser fundamental para futuras decisões de casos envolvendo o "uso indevido de dados", assim como para o desenvolvimento de um regime de proteção de dados pessoais que considere as particularidades econômicas, sociais e políticas locais e que esteja alinhada com as garantias e os direitos fundamentais já consagrados pelo nosso ordenamento.

REFERÊNCIAS

BAMBERGER, Kenneth A.; MULLIGAN, Deirdre K. Privacy on the Books and on the Ground. **Stanford Law Review**, v. 63, n. 2, p. 247-316, 2010.

BENJAMIN, Antônio Herman de Vasconellos. Arts. 29 a 45: Seção VI – Dos bancos de dados e cadastros de consumidores. In: GRINOVER, Ada Pellegrini. **Código Brasileiro de Defesa do Consumidor**: comentado pelos autores do anteprojeto. 9. ed. Rio de Janeiro: Forense Universitária, 2007. p. 410-503.

BENNETT, Colin J.; RAAB, Charles D. Revisiting the governance of privacy: Contemporary policy instruments in global perspective. **Regulation & Governance**, v. 14, n. 3, p. 447-464, 2020. Disponível em: https://doi.org/10.1111/rego.12222.

BIONI, B. Compreendendo o conceito de anonimização e dado anonimizado. **Cadernos Jurídicos**, São Paulo, v. 53, p. 191-201, nov. 2020.

BIONI, B. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2018.

BIONI, B. et al. **Xeque-mate**: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: GPoPAI/USP, 2015.

BIONI, B.; PIGATTO, J. **A Autoridade Nacional de Proteção de Dados e o possível ingresso do Brasil na OCDE**. Observatório – por Data Privacy Brasil, 4 nov. 2020. Disponível em: https://observatorioprivacidade.com.br/2020/11/04/a-autoridade-nacional-de-protecao-de-dados-e-o-possivel-ingresso-do-brasil-na-ocde/. Acesso em: 27 jan. 2021.

BOOTH, W. C. et al. **A arte da pesquisa**. 3. ed. São Paulo: Martins Fontes, 2019.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 24 nov. 2021.

BRASÍLIA. Secretaria Nacional do Consumidor. Ministério da Justiça e Segurança Pública. **ANPD e Senacon assinam acordo de cooperação técnica**. 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-senacon-assinam-acordo-de-cooperacao-tecnica. Acesso em: 24 nov. 2021.

BRASÍLIA. Secretaria Nacional do Consumidor. Ministério da Justiça e Segurança Pública. **Biblioteca: notas técnicas**. Disponível em: https://www.defesadoconsumidor.gov.br/portal/biblioteca/95-notas-tecnicas. Acesso em: 24 nov. 2021.

BRASÍLIA. Secretaria Nacional do Consumidor. Ministério da Justiça e Segurança Pública. **Ministério da Justiça e Segurança Pública lança campanha educativa para informar consumidor sobre proteção de dados**. 2021. Disponível em: https://www.defesadoconsumidor.gov.br/portal/ultimas-noticias/1901-ministerio-da-justica-e-seguranca-publica-lanca-campanha-educativa-para-informar-consumidor-sobre-protecao-de-dados. Acesso em: 24 nov. 2021.

BRASÍLIA. Secretaria Nacional do Consumidor. Ministério da Justiça e Segurança Pública. **Secretaria Nacional do Consumidor se reúne com ANPD para tratar de acordo para proteção de dados dos consumidores**. 2021. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/secretaria-nacional-do-consumidor-se-reune-com-anpd-para-tratar-de-acordo-para-protecao-de-dados-dos-consumidores. Acesso em: 24 nov. 2021.

BRYANT, Antony; CHARMAZ, Kathy. **The SAGE Handbook of Current Developments in Grounded Theory**. 55 City Road, London, 2021.

CAMAROTTO, Murillo. Uso de empresas de fachada para venda ilegal de dados entra na mira do governo. **Valor Econômico**, Brasília, p. 1-2, 24 set. 2020. Disponível em: https://valor.globo.com/brasil/noticia/2020/09/24/uso-de-empresas-de-fechada-para-venda-ilegal-de-dados-entra-na-mira-do-governo.ghtml. Acesso em: 2 nov. 2021.

CAPPI, Riccardo. A "Teorização Fundamentada nos Dados": um método possível na pesquisa empírica em direito. *In*: MACHADO, Maíra Rocha (org.). **Pesquisar empiricamente o direito**. São Paulo: Rede de Estudos Empíricos em Direito, 2017.

CHARMAZ, Kathy. **Constructing Grounded Theory**. London; Thousand Oaks, Calif: Sage Publications Ltd, 2006.

COALIZÃO DIREITOS NA REDE. **Vigência da LGPD e os desafios na implementação da ANPD e do CNPD**. 4 set. 2020. Disponível em: https://direitosnarede.org.br/2020/09/04/vigencia-da-lgpd-e-os-desafios-na-implementacao-da-anpd-e-do-cnpd/. Acesso em: 21 fev. 2021.

CROTTY, Michael. **The foundations of social research**: meaning and perspective in the research process. London: Routledge, 1998.

DATA PRIVACY BRASIL. **DPBR Live – Proteção de Dados e Direitos do Consumidor**. São Paulo, 2020. Disponível em: https://www.youtube.com/watch?v=0P3aB8DCwL4. Acesso em: 21 fev. 2021.

DATA PRIVACY BRASIL. **Memória da LGPD**. Observatório da Privacidade e Proteção de dados. Disponível em: https://observatorioprivacidade.com.br/memorias/. Acesso em: 20 fev. 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Revista dos Tribunais, 2019.

EUROPE. European Commission. **Communication from The Commission to The European Parliament, The Council, The Economic and Social Committee and The Committee of the Regions**. 2010. Disponível em: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF. Acesso em: 16 dez. 2021.

GERBER, N.; GERBER, P.; VOLKAMER, M. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. **Computers & Security**, v. 77, p. 226-261, ago. 2018.

HUSTINX, P. The reform of EU data protection: towards more effective and more consistent data protection across the EU. *In*: WITZLEB, N. et al. (eds.). **Emerging Challenges in Privacy Law**. Cambridge: Cambridge University Press, 2014. p. 62-72.

KIRBY, M. The history, achievement and future of the 1980 OECD guidelines on privacy. **International Data Privacy Law**, v. 1, n. 1, p. 6-14, 1 fev. 2011. Disponível em: https://academic.oup.com/idpl/article/1/1/6/759637. Acesso em: 16 dez. 2021.

LEORATTI, A.; PIMENTA, G. Autoridade de proteção de dados: Cade sugere mudar lei para ser ANPD. **JOTA Info**, 17 ago. 2020. Disponível em: https://www.jota.info/tributos-e-empresas/concorrencia/autoridade-de-protecao-de-dados-cade-17082020. Acesso em: 27 jan. 2021.

MAYER-SCHONEBERGER, Viktor. Generational development of data protection in Europe. *In*: AGRE, Phillip E.; ROTENBERG Marc (org.). **Technology and privacy**: the new landscape. Cambridge, MA: The MIT Press, 1997.

PRADO, M. M. **What is Law and Development?** Rochester, NY: Social Science Research Network, 1 out. 2010. Disponível em: https://papers.ssrn.com/abstract=1907298. Acesso em: 23 out. 2021.

SECRETARIA NACIONAL DO CONSUMIDOR. **Sistema Nacional de Informações de Defesa do Consumidor – SINDEC**. Disponível em: https://sindecnacional.mj.gov.br/sobre. Acesso em: 5 dez. 2021.

SENADO FEDERAL. Sancionada com vetos Lei Geral de Proteção de Dados Pessoais. **Senado Notícias**, 15 ago. 2018. Disponível em: https://www12.senado.leg.br/noticias/materias/2018/08/15/sancionada-com-vetos-lei-geral-de-protecao-de-dados-pessoais. Acesso em: 20 fev. 2021.

SERUR ADVOGADOS. **O papel dos conselhos consultivos de agências reguladoras e do conselho nacional de proteção de dado**. Brasília, 2021. Color. Disponível em: https://www.youtube.com/watch?v=bMdhhXJ63K4. Acesso em: 24 nov. 2021.

SIMÃO, Barbara; MORIBE, Gabriela. **Quem aplica e atesta o direito**: o ensino jurídico e as certificações em proteção de dados. 2021. No prelo.

STRAUSS, A. L.; CORBIN, J. M. **Basics of qualitative research**: techniques and procedures for developing grounded theory. 2. ed. Thousand Oaks: Sage Publications, 2008.

SUNSTEIN, Cass; VERMEULE, Adrian. Interpretation and Institutions. **Michigan Law Review**, v. 101, n. 4, p. 885-951, 2003.

TAYLOR, L.; VAN DER SLOOT, B.; FLORIDI, L. Conclusion: What Do We Know About Group Privacy? *In*: TAYLOR, L.; FLORIDI, L.; VAN DER SLOOT, B. (eds.). **Group Privacy**: New Challenges of Data Technologies. Philosophical Studies Series. Cham: Springer International Publishing, 2017. p. 225-237.

TENE, O. Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws. **Ohio State Law Journal**, v. 74, p. 1217, 2013. Disponível em:

https://heinonline.org/HOL/Page?handle=hein.journals/ohslj74&id=1255&div=&collection=. Acesso em: 16 dez. 2021.

TIMM, Luciano Benetti. Conselho Nacional de Defesa do Consumidor: um espaço institucional de interlocução de políticas públicas nacionais. **O Estadão**, São Paulo, 16 jul. 2020. Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/conselho-nacional-de-defesa-do-consumidor-um-espaco-institucional-de-interlocucao-de-politicas-publicas-nacionais/. Acesso em: 14 dez. 2021.

UNIÃO EUROPEIA. Parlamento Europeu. (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with the regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 14 ago. 2021.

WILLIAMS, Raymon. **Palavras-chave**: um vocabulário de cultura e sociedade. São Paulo: Boitempo, 2007.

WIMMER, Miriam. **Interfaces entre proteção de dados pessoais e segurança da informação**: um debate sobre a relação entre Direito e Tecnologia. 2019. No prelo.

ZUBOFF, S. **The age of surveillance capitalism**: the fight for a human future at the new frontier of power. New York: PublicAffairs, 2018.

APÊNDICE A – Relação das notas técnicas analisadas, em ordem cronológica

Número da nota técnica	Data	Representada	Tipo	Ementa
Nota Técnica nº 33/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	06/02/2019	Google Brasil Internet Ltda.	Averiguação Preliminar Processo nº 08012.004630/2015-11	"Averiguação preliminar. Termos de Uso. Ausência de destaque para a prática de escaneamento de conteúdo de e-mails. Suposto descumprimento do dever de informar. Relação de consumo. Marco Civil da Internet. Provável violação a dispositivo que prescreve o destaque para cláusula que preveja coleta e tratamento de dados pessoais. Sugestão de instauração de processo administrativo."
Nota Técnica nº 108/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	11/03/2019	Facebook Inc. e Facebook Serviços Online do Brasil Ltda.	Averiguação Preliminar Processo nº 08012.000723/2018-19	"Averiguação preliminar. Suposto desvio de tráfego de internet para fins publicitários. Prática abusiva. Publicidade abusiva. Sugestão de instauração de processo administrativo."
Nota Técnica nº 109/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	11/03/2019	Facebook Inc. e Facebook Serviços Online do Brasil Ltda.	Averiguação Preliminar Processo nº 08012.002467/2018-02	"Averiguação preliminar. Suposta invasão de contas de usuários brasileiros por hackers para coleta de dados pessoais. Prática abusiva. Violação ao dever de segurança. Sugestão de instauração de processo administrativo."

Nota Técnica nº 243/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	18/07/2019	Banco BMG S.A.	Averiguação Preliminar Processo nº 08012.001478/2019-48	"Averiguação Preliminar. Supostas abusividades na oferta e concessão de empréstimos consignados por instituição financeira. Abordagem por telefone de idosos aposentados e pensionistas do INSS. Possível exploração da hiper vulnerabilidade do idoso. Indícios de prática de abusos na oferta e de violação de dados pessoais do idoso. Sugestão de Instauração de Processo Administrativo."
Nota Técnica nº 231/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	18/07/2019	Caixa Econômica Federal	Averiguação Preliminar Processo nº 08012.001492/2019-41	"Averiguação Preliminar. Supostas abusividades na oferta e concessão de empréstimos consignados por instituição financeira. Abordagem por telefone de idosos aposentados e pensionistas do INSS. Possível exploração da hiper vulnerabilidade do idoso. Indícios de prática de abusos na oferta e de violação de dados pessoais do idoso. Sugestão de Instauração de Processo Administrativo."
Nota Técnica nº 242/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	18/07/2019	Banco Safra S.A.	Averiguação Preliminar Processo nº 08012.001486/2019-94	"Averiguação Preliminar. Supostas abusividades na oferta e concessão de empréstimos consignados por instituição financeira. Abordagem por telefone de idosos aposentados e pensionistas do INSS. Possível exploração da hiper

				vulnerabilidade do idoso. Indícios de prática de abusos na oferta e de violação de dados pessoais do idoso. Sugestão de Instauração de Processo Administrativo.”
Nota Técnica nº 244/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	18/07/2019	Banco Olé Bonsucesso Consignado S/A	Averiguação Preliminar Processo nº 08012.001483/2019-51	“Averiguação Preliminar. Supostas abusividades na oferta e concessão de empréstimos consignados por instituição financeira. Abordagem por telefone de idosos aposentados e pensionistas do INSS. Possível exploração da hiper vulnerabilidade do idoso. Indícios de prática de abusos na oferta e de violação de dados pessoais do idoso. Sugestão de Instauração de Processo Administrativo.”
Nota Técnica nº 245/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	18/07/2019	Banco Itaú Consignado S.A.	Averiguação Preliminar Processo nº 08012.001470/2019-81	“Averiguação Preliminar. Supostas abusividades na oferta e concessão de empréstimos consignados por instituição financeira. Abordagem por telefone de idosos aposentados e pensionistas do INSS. Possível exploração da hiper vulnerabilidade do idoso. Indícios de prática de abusos na oferta e de violação de dados pessoais do idoso. Sugestão de Instauração de Processo Administrativo.”

Nota Técnica nº 246/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	18/07/2019	Banco do Estado do Rio Grande do Sul S.A.	Averiguação Preliminar Processo nº 08012.001490/2019-52	"Averiguação Preliminar. Supostas abusividades na oferta e concessão de empréstimos consignados por instituição financeira. Abordagem por telefone de idosos aposentados e pensionistas do INSS. Possível exploração da hiper vulnerabilidade do idoso. Indícios de prática de abusos na oferta e de violação de dados pessoais do idoso. Sugestão de Instauração de Processo Administrativo."
Nota Técnica nº 247/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	18/07/2019	Banco Pan S.A.	Averiguação Preliminar Processo nº 08012.001462/2019-35	"Averiguação Preliminar. Supostas abusividades na oferta e concessão de empréstimos consignados por instituição financeira. Abordagem por telefone de idosos aposentados e pensionistas do INSS. Possível exploração da hiper vulnerabilidade do idoso. Indícios de prática de abusos na oferta e de violação de dados pessoais do idoso. Sugestão de Instauração de Processo Administrativo."
Nota Técnica nº 248/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	18/07/2019	Banco Cetelem S.A.	Averiguação Preliminar Processo nº 08012.001476/2019-59	"Averiguação Preliminar. Supostas abusividades na oferta e concessão de empréstimos consignados por instituição financeira. Abordagem por telefone de idosos aposentados e pensionistas do INSS. Possível exploração da hiper

				vulnerabilidade do idoso. Indícios de prática de abusos na oferta e de violação de dados pessoais do idoso. Sugestão de Instauração de Processo Administrativo.”
Nota Técnica nº 249/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	18/07/2019	Banco Bradesco Financiamentos S.A.	Averiguação Preliminar Processo nº 08012.001488/2019-83	“Averiguação Preliminar. Supostas abusividades na oferta e concessão de empréstimos consignados por instituição financeira. Abordagem por telefone de idosos aposentados e pensionistas do INSS. Possível exploração da hiper vulnerabilidade do idoso. Indícios de prática de abusos na oferta e de violação de dados pessoais do idoso. Sugestão de Instauração de Processo Administrativo.”
Nota Técnica nº 250/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	18/07/2019	Banco Bradesco S.A.	Averiguação Preliminar Processo nº 08012.001489/2019-28	“Averiguação Preliminar. Supostas abusividades na oferta e concessão de empréstimos consignados por instituição financeira. Abordagem por telefone de idosos aposentados e pensionistas do INSS. Possível exploração da hiper vulnerabilidade do idoso. Indícios de prática de abusos na oferta e de violação de dados pessoais do idoso. Sugestão de Instauração de Processo Administrativo.”

Nota Técnica nº 294/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	30/08/2019	Cia Hering	Averiguação Preliminar Processo nº 08012.001387/2019-11	"Averiguação Preliminar. Suposta utilização de tecnologia para a coleta de dados de consumidores sem conhecimento prévio e consentimento. Possível prática abusiva e violação de princípios e direitos do Código de Defesa do Consumidor. Sugestão de instauração de processo administrativo."
Nota Técnica nº 310/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	12/09/2019	Tim Celular S.A.	Averiguação Preliminar Processo nº 08012.001392/2019-15	"Averiguação preliminar. Suposto vazamento de dados pessoais de consumidores. Proteção à privacidade. Possível prática abusiva por exposição de dados de consumidores. Indícios de ofensa aos princípios da vulnerabilidade, da transparência, da confiança, da educação, da informação, da harmonização de interesse e da boa-fé, além dos direitos de liberdade de escolha, informação adequada, proteção contra práticas abusivas e efetiva prevenção e reparação de danos. Respeito ao tratamento de dados dos consumidores. Responsabilidade objetiva da operadora de telefonia. Sugestão de instauração de processo administrativo."

Nota Técnica nº 362/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	16/10/2019	Facebook Inc. e Facebook Serviços Online do Brasil Ltda.	Averiguação Preliminar Processo nº 08012.000520/2019-11	"Averiguação preliminar. Suposto compartilhamento indevido e sem consentimento de dados sensíveis de consumidores para fins publicitários. Prática abusiva. Publicidade abusiva. Sugestão de instauração de processo administrativo."
Nota Técnica nº 379/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	24/10/2019	Ns2. Com Internet S.A.	Averiguação Preliminar Processo nº 08012.000145/2018-11	"Averiguação preliminar. Exposição de dados pessoais de consumidores. Proteção à privacidade. Possível prática abusiva por exposição de dados de consumidores. Celebração de Termo de Ajustamento de Conduta (TAC) com o Ministério Público do Distrito Federal e Territórios (MPDFT). Exaurimento de finalidade. Sugestão de arquivamento."
Nota Técnica nº 407/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	28/11/2019	Google Brasil Internet Ltda.	Averiguação Preliminar Processo nº 08012.002781/2019-68	"Averiguação Preliminar. Suposta coleta de dados de crianças, sem o devido consentimento, para fins publicitários. Possível prática abusiva e violação de princípios e direitos do Código de Defesa do Consumidor. Sugestão de instauração de processo administrativo."
Nota Técnica nº 378/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	24/12/2019	J&A Holding Ltda.	Averiguação Preliminar Processo nº 08012.001400/2019-23	"Suposto vazamento de dados pessoais de consumidores. Proteção à privacidade. Possível prática abusiva por

				comercialização de dados de consumidores. Não localização da pessoa jurídica. Provável extinção. Perda de objeto. Sugestão de arquivamento.”
Nota Técnica nº 32/2019/CGCTSA/DPDC/SENACON/MJ	27/12/2019	Facebook Inc. e Facebook Serviços Online do Brasil Ltda.	Processo Administrativo nº 08012.000723/2018-19	“Processo Administrativo. Infração aos direitos básicos do consumidor no que diz respeito ao reconhecimento de sua vulnerabilidade, ausência de boa-fé, ao equilíbrio entre consumidores e fornecedores, ao direito à privacidade e à intimidade. Cometimento de prática abusiva em desfavor da coletividade consumerista. Falha no dever de fornecimento de informações claras e adequadas quanto a sua política de privacidade pelas Representadas. Falha na custódia adequada dos dados fornecidos pelos usuários considerando o modelo de negócios adotado. Descumprimento dos artigos 4º, *caput*, I, III e IV; 6º, II, III, IV e VI, art. 18, art. 31; art. 37 e art. 39, todos do Código de Defesa do Consumidor, além das disposições do Marco Civil da Internet, notadamente, os arts. 2º, inc. II e III, e 7º, incs. VI, VII, VIII, IX e XIII. Sugestão de aplicação de sanção

				de multa no valor de R$ 6.600.000,00 (seis milhões e seiscentos mil reais).”
Nota Técnica nº 19/2020/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	26/03/2020	C&A Modas S.A.	Averiguação Preliminar Processo nº 08012.002376/2017-88	“Averiguação Preliminar. Suposta prática abusiva. Exposição de dados dos consumidores. Exaurimento de finalidade.”
Nota Técnica nº 395/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	14/05/2020	Sky Serviços de Banda Larga Ltda.	Averiguação Preliminar Processo nº 08012.003074/2018-16	“Averiguação preliminar. Exposição temporária. Arquivos de logs. Proteção à privacidade. Possível prática abusiva. Atuação proativa da SKY para resolver o problema. Contratação de empresa independente. Entendimento do MPDFT no sentido de ausência de demonstração de exposição de dados de consumidores e de suficiência das providências adotadas. Exaurimento de finalidade. Sugestão de Arquivamento.”
Nota Técnica nº 42/2020/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	30/06/2020	Química Amparo Ltda.	Averiguação Preliminar Processo nº 08000.030856/2019-30	“Informação. Prestação de esclarecimentos pela empresa interessada de vazamento de dados pessoas de consumidores inscritos em ato promocional. Criação de portal para esclarecimento a consumidores. Investigação mediante empresas independentes. Identificação dos agentes violadores mediante ação judicial. Não

				revelação de danos em decorrência do incidente. Sugestão de arquivamento.”
Nota Técnica nº 10/2020/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	21/07/2020	Facebook Serviços Online do Brasil Ltda. C/C Facebook Inc.	Averiguação Preliminar Processo nº 08012.002596/2019-73	“Averiguação preliminar. Facebook. Transcrição de áudios de usuários sem autorização. Recurso de ‘voz para texto’ foi disponibilizado pelo Facebook Inc. aos usuários do Messenger localizados nos Estados Unidos da América, estando assim disponível apenas no e para o idioma inglês. Ausência de impacto da infração no Brasil. Sugestão de arquivamento.”
Nota Técnica nº 8/2020/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	30/07/2020	Mercedes-Benz do Brasil Ltda.	Averiguação Preliminar Processo nº 08012.002762/2019-31	“Averiguação Preliminar. Reportagem denominada ‘Como a Mercedes persegue os clientes que não pagam’, segundo a qual houve utilização do *e-call* na Europa, de forma indevida, com a finalidade de rastrear consumidores inadimplentes. Ausência de elementos para prosseguir com a investigação. Exaurimento de finalidade. Sugestão de Arquivamento.”
Nota Técnica nº 62/2020/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	13/08/2020	Cia Hering	Processo Administrativo nº 08012.001387/2019-11	“Processo Administrativo. Utilização de tecnologia para a coleta de dados de consumidores sem conhecimento prévio e consentimento. Prática abusiva e violação de princípios e direitos do Código de Defesa

				do Consumidor. Infração aos artigos 4º, incisos I e III; 6º, incisos II, III, IV e VI; 39, IV; e 43 do Código de Defesa do Consumidor. Aplicação de sanção de multa no valor de R$ 58.767,00 (cinquenta e oito mil setecentos e sessenta e sete reais).”
Nota Técnica nº 67/2020/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	13/08/2020	Zoom Video Communications Inc.	Averiguação Preliminar Processo nº 08012.000760/2020-41	“Averiguação Preliminar. Suposta prática abusiva. Exposição de dados de consumidores. Exaurimento de finalidade. Arquivamento.”
Nota Técnica nº 75/2020/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	24/08/2020	Facebook Inc. e Facebook Serviços Online do Brasil Ltda.	Averiguação Preliminar Processo nº 08012.001086/2019-89	“Averiguação preliminar. Suposta exposição de dados da plataforma do Facebook por desenvolvedores de aplicativos contratados pelo Facebook. ausência de indícios sobre consumidores localizados neste país terem sido afetados significativamente pelo evento. Sugestão de arquivamento.”
Nota Técnica nº 35/2021/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	27/05/2021	Banco Pan S.A.	Processo Administrativo nº 08012.001462/2019-35	“Procedimento administrativo sancionador. Conduta abusiva na oferta e concessão de empréstimos consignados por instituição financeira. Abordagem nociva por telefone de idosos aposentados e pensionistas do INSS. Exploração da hiper vulnerabilidade do idoso. Práticas abusivas na oferta de

				empréstimos consignados: ausência de informação clara e adequada e violação de dados pessoais de idosos. Violação aos artigos 4º, *caput*, I e III; 6º, incisos II, III e IV; 39, inciso IV; 43 (*caput* e parágrafos) do Código de Defesa do Consumidor e aos arts. 7º, incs. I, VII, VIII, IX, X, 10, *caput* e § 1º, e 11, do Marco Civil da Internet. Sugestão de aplicação de sanção administrativa de multa no valor de R$ 8.800.000,00 (oito milhões e oitocentos mil reais)."
Nota Técnica nº 28/2021/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	10/06/2021	Banco Cetelem S.A.	Processo Administrativo nº 08012.001476/2019-59	"Procedimento administrativo sancionador. Conduta abusiva na oferta e concessão de empréstimos consignados por instituição financeira. Abordagem nociva por telefone de idosos aposentados e pensionistas do INSS. Exploração da hiper vulnerabilidade do idoso. Práticas abusivas na oferta de empréstimos consignados: ausência de informação clara e adequada e violação de dados pessoais de idosos. Violação aos artigos 4º, *caput*, I e III; 6º, incisos II, III e IV; 39, inciso IV; 43 (*caput* e parágrafos) do Código de Defesa do Consumidor e aos arts. 7º, incs. I, VII, VIII, IX, X, 10, *caput* e § 1º, e 11, do Marco Civil da Internet. Sugestão

				de aplicação de sanção administrativa de multa no valor de R$ 4.000.000,00 (quatro milhões de reais).”
Nota Técnica nº 40/2021/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	21/06/2021	Banco Itaú Consignado S.A.	Processo Administrativo nº 08012.001470/2019-81	“Procedimento administrativo sancionador. Conduta abusiva na oferta e concessão de empréstimos consignados por instituição financeira. Abordagem nociva por telefone de idosos aposentados e pensionistas do INSS. Exploração da hiper vulnerabilidade do idoso. Práticas abusivas na oferta de empréstimos consignados: ausência de informação clara e adequada sobre a abertura de cadastro, ausência de consentimento do titular e violação de dados pessoais de idosos. Violação aos artigos 4º, *caput*, I e III; 6º, incisos II, III e IV; 39, inciso IV; 43 (*caput* e parágrafos) do Código de Defesa do Consumidor e aos arts. 7º, incs. I, VII, VIII, IX, X, 10, *caput* e § 1º, e 11, do Marco Civil da Internet. Sugestão de aplicação de sanção administrativa de multa no valor de R$ 9.600.000,00 (nove milhões seiscentos mil reais).”
Nota Técnica nº48/2021/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	30/06/2021	Banco BMG S.A.	Processo Administrativo nº 08012.001478/2019-48	“Procedimento administrativo sancionador. Conduta abusiva na oferta e concessão de produtos consignados por instituição

				financeira. Abordagem nociva de idosos aposentados e pensionistas do INSS. Exploração da hiper vulnerabilidade do idoso. Práticas abusivas na oferta de produtos consignados: ausência de informação clara e adequada sobre abertura de bancos de dados de titulares e obtenção de dados pessoais de idosos sem o devido consentimento. Violação aos artigos 4º, *caput*, I e III; 6º, incisos II, III e IV; 39, inciso IV; 43 (*caput* e parágrafos) do Código de Defesa do Consumidor e aos arts. 7º, incs. I, VII, VIII, IX, X, 10, *caput* e § 1º, e 11, do Marco Civil da Internet. Sugestão de aplicação de sanção administrativa de multa no valor de R$ 5.100.000,00 (cinco milhões cem mil reais).”
Nota Técnica nº 56/2021/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ	14/07/2021	Banco Safra S.A.	Processo Administrativo nº 08012.001486/2019-94	“Procedimento administrativo sancionador. Conduta abusiva na oferta e concessão de empréstimos consignados por instituição financeira. Abordagem nociva de idosos aposentados e pensionistas do INSS. Exploração da hiper vulnerabilidade do idoso. Práticas abusivas na oferta de empréstimos consignados: ausência de informação clara e adequada e violação de

dados pessoais de idosos. Violação aos artigos 4º, *caput*, I e III; 6º, incisos II, III e IV; 39, inciso IV; 43 (*caput* e parágrafos) do Código de Defesa do Consumidor e aos arts. 7º, incs. I, VII, VIII, IX, X, 10, *caput* e § 1º, e 11, do Marco Civil da Internet. Sugestão de aplicação de sanção administrativa de multa no valor de R$ 2.400.000,00 (dois milhões quatrocentos mil reais).”
