

A ADMINISTRAÇÃO PÚBLICA E A PROTEÇÃO DE DADOS PESSOAIS: O DESAFIO DA PRIVACIDADE NO ÂMBITO DA SEGURIDADE SOCIAL

Ana Carolina Ferreira de Moraes e Ana Cláudia Silva Scalquette

Apoio: PIBIC CNPq

RESUMO

Os dados pessoais tornaram-se parte indispensável da sociedade da informação em que vivemos hoje. O seu tratamento permeia uma gama ampla de atividades da vida humana, de modo que a informação se tornou essencial para o desenvolvimento de produtos e o para continuidade da prestação de serviços. Acontece que esses dados, enquanto elementos capazes de identificar e individualizar uma pessoa, acabam por representá-la quase que completamente. Por conseguinte, tornam-se extensão da sua própria personalidade, podendo revelar muitos aspectos da vida privada quando tratados. É nesse ponto que se revela a existência do risco de violação da privacidade dos titulares de dados pessoais, bem como de sua personalidade, afetando a sua existência digna. Além disso, em decorrência das inegáveis benesses geradas pelo uso dos dados pessoais e a aplicação de tecnologias da informação, não só as empresas privadas como o Estado tem caminhado em direção implementar a utilização dos dados pessoais para melhorar a eficiência e a eficácia dos serviços que prestam. As entidades e órgãos que compõem a Seguridade Social no Brasil, por exemplo, tem trabalhado para desenvolver sistemas informáticos, a fim de tornar mais prático o fornecimento de serviços públicos atinentes a saúde, previdência e assistência social. Tendo em consideração esse cenário, é necessário abrir um debate acerca das implicações do tratamento de dados pessoais na realidade e como o direito precisará ser adequar para responder aos novos conflitos dele decorrentes.

Palavras-chave: dados, privacidade, Seguridade

1. INTRODUÇÃO

Os dados pessoais informatizados representam para a sociedade atual um recurso com alto valor porque abrem uma gama de novas possibilidades de exploração das tecnologias da informação para tornar mais eficaz os processos produtivos e mais proveitosos os serviços. O seu tratamento se tornou parte imprescindível das mais variadas atividades humanas, ainda mais porque instrumentos como o *big data* ou a inteligência artificial permitiram que a coleta, o armazenamento e a interpretação de dados se desse de forma rápida e barata.

Assim como as empresas privadas, o Poder Público percebeu esse indiscutível progresso que a incorporação do uso informatizado dos dados pessoais poderia trazer, especialmente para áreas estratégicas como a saúde e a segurança pública (VENTURINI, 2016). Durante a pandemia de covid-19, por exemplo, a integração dos sistemas informáticos e dos bancos de dados de saúde foi essencial para a gestão de estratégias de enfrentamento a doença.

Contudo, o que também se observou nesse período foi a dificuldade da Administração Pública em manejar e proteger os dados pessoais sob sua tutela. Conforme será explorado mais a frente, os anos de 2020 e 2021 foram marcados por notícias de falhas no sistemas do Ministério da Saúde e pelo vazamento dos dados pessoais dos cidadãos brasileiros.

Esse problema também pode ser observado na previdência social. Há pelo menos sete anos (CASTELANI; BRIGATTI, 2015) já existem notícias sobre o vazamento de dados pessoais de segurados do Regime Geral da Previdência Social, dados esses que eram, inclusive, usados para prática de publicidade abusiva por instituições financeiras e até mesmo como instrumentos para fraudar o INSS.

Tendo em mente esse contexto, é preciso ressaltar que a quantidade de dados pessoais coletados nessas áreas é bastante volumosa e inclui dados categorizados como sensíveis. Consequentemente, as entidades nelas atuantes precisam estar preparadas para lidar com o risco de violação da privacidade e da personalidade do titular do dado pessoal, visto que enquanto parte da sua identificação e individualização funcionam como uma extensão da sua personalidade.

Em razão disso, o presente estudo pretende identificar com quais falhas a Administração Pública tem lidado no tratamento de dados no âmbito da Seguridade Social e em que medida tem protegido a privacidade dos administrados a partir das reações do mundo jurídico as falhas amplamente divulgadas na imprensa. Cabe destacar que a escolha pela análise a partir da perspectiva da Seguridade Social se deu porque esse

sistema inclui a execução de serviços públicos na saúde, previdência e assistência social, áreas que requerem o tratamento de um número considerável de dados pessoais e que impactam diretamente na qualidade de vida da população.

2. A SEGURIDADE SOCIAL E A PRIVACIDADE NO TRATAMENTO DE DADOS PESSOAIS

2.1 A relevância do tratamento de dados pessoais para a Seguridade Social

A Seguridade Social, delineada no art. 194 da Constituição Federal, é um sistema desenvolvido como um instrumento de realização dos direitos sociais da saúde, assistência e previdência social (CORREIA; CORREIA, 2002, p. 17), expressamente previstos no seu art. 6º. Esses direitos fazem parte de um complexo de proteção que o legislador constituinte entendeu necessário para a garantia da dignidade da pessoa humana, um dos fundamentos da própria República Federativa do Brasil (BRASIL, 1988). Do mesmo modo, é imprescindível à consecução dos objetivos impostos pela Carta Magna no art. 3º, especialmente com relação a erradicação da pobreza e marginalização, redução desigualdade sociais e regionais e a promoção do bem de todos.

Em outras palavras, a Seguridade foi pensada para que o Estado executasse ações aptas a estender a toda a população as condições necessárias para a sua manutenção de forma digna. Em outras palavras:

A inclusão da previdência, da saúde e da assistência como partes da seguridade social, introduz a noção de direitos sociais universais como parte da condição de cidadania, sendo que antes eram restritos à população beneficiária da previdência. O novo padrão constitucional da política social caracteriza-se pela universalidade na cobertura, o reconhecimento dos direitos sociais, a afirmação do dever do estado, a subordinação das práticas privadas à regulação em função da relevância pública das ações e serviços nestas áreas, uma perspectiva publicista de co-gestão governo/sociedade, um arranjo organizacional descentralizado. (FLEURY, 2017)

À título de exemplo, o art. 7º da Constituição Federal determina um rol de direitos de trabalhadores rurais e urbanos que visam a melhoria da sua condição social, muitos dos quais são realizados pela Seguridade Social. É o caso da aposentadoria, licença maternidade e seguro contra acidente de trabalho, todos de execução gerenciada e regulamentada no âmbito previdenciário.

Diante disso e considerando que o “[...] Estado contemporâneo possui, entre suas funções, a proteção social dos indivíduos em relação a eventos que lhes possam causar a dificuldade ou até mesmo a impossibilidade de subsistência por conta própria [...]” (LAZZARI; CASTRO, 2021, p. 46-49), exige-se do Poder Público a coordenação da

atuação estatal em todos os âmbitos para criar a estrutura necessária a fim de operacionalizar a saúde, a previdência e a assistência social. Isto significa que, requer-se a execução de uma gama variada de atividades e a atuação coordenada de muitos agentes diferentes para oferecer com eficácia e eficiência os serviços concernentes a essas áreas. Por essa razão, quando da promulgação da Constituição de 1988 que trazia como uma das novidades o sistema da Seguridade Social, Wagner Balera (1989) a respeito do tema destacou que:

A articulação dessas estruturas é tarefa das mais complexas. Envolve uma multiplicidade de órgãos, de práticas, de técnicas e um arcabouço normativo que se espalha por todos os níveis de Poder: o Federal, o Estadual, o Municipal e, mais ainda, por distintos regimes de proteção existentes num mesmo nível.

Nessas circunstâncias, o tratamento de dados pessoais tem sido uma ferramenta essencial para a criação e manutenção de muitos serviços oferecidos e utilizados por entidades públicas e privadas (LOTT; CIANCONI, 2018a, P. 117-132). Os entes governamentais, por exemplo, continuamente investem no desenvolvimento de tecnologias da informação capazes de coletar e tratar uma quantidade massiva de dados (TAPAJÓS, 1999, p. 53-63) referentes a população brasileira, de forma a possibilitar o alcance dos serviços públicos a uma camada maior da população. Com todos os dados coletados e as inferências que os sistemas automatizados são capazes de fazer, esses serviços podem ser executados com mais celeridade e efetividade, uma vez que são pensados e instrumentalizados a partir de informações precisas acerca do grupo alvo. Tanto que, conforme explicam Yuri Monnerat Lott e Regina de Barros Cianconi (2018b, p. 117-132):

A grande questão que move as empresas e os governos para o big data é a (nova) possibilidade de encontrar relações entre pontos distantes de um sistema complexo e sem necessariamente entender suas causas, podendo fazer previsões para o futuro. Os big data-esses conjuntos de dados massivos que advêm de situações reais são extremamente complexos e impossíveis de serem interpretados pela mente humana, fato que trouxe novos e poderosos métodos de análise a partir de algoritmos e uso de inteligência artificial por meio da aprendizagem de máquina (machine learning).

Para compreender essa realidade, cumpre elucidar que o objeto desse procedimento a que se chama tratamento é o dado, que traz alguma informação sobre um determinado

evento ou sobre uma pessoa¹. O que o tornará pessoal é o vínculo objetivo que tem com o seu titular, caracterizado pela atribuição que a informação dá sobre algum aspecto do indivíduo (COSTA, 2021, p. 89-102). Seguindo esse raciocínio, quando ocorre a ruptura desse vínculo entre determinado atributo e o seu titular a partir da aplicação de técnicas durante o seu tratamento, estar-se-á diante de dado anônimo, ou seja, uma informação que não poderá identificar o seu titular. O dado pessoal sensível, por sua vez, é uma categoria de dado pessoal que envolve um atributo com de alto potencial discriminatório, tendo em vista que carrega informações com conotações socialmente negativas hábeis a possibilitar a segregação de determinados grupos (DONEDA, 2019, p. 142). Em outras palavras, será sensível o dado que carrega caracteres imanescentes a personalidade do sujeito (MIRANDA, 2016, p. 105). Estipular a qual categoria certo dado pertence é essencial para definir quais serão as normas jurídicas que regerão o seu tratamento. Isto é, a depender do tipo de dado a ser operado as regras possuirão limitações legais de maior ou menor grau.

Isto posto, pode-se dizer que o tratamento de dados pessoais nada mais é do que o processo pelo qual uma informação fornecida pelo seu titular ganha utilidade através da aplicação de métodos e técnicas.

Tendo em mente essas circunstâncias, o Estado quando da execução de ações na área da Seguridade Social assume a posição de agente de tratamento. Isso significa que, para desenvolver políticas públicas para a saúde, assistência e previdência social, inúmeras vezes o Poder Público trata os dados pessoais da população brasileira e toma decisões quanto a esse tratamento.

Acerca disso, interessante mencionar o Conecte SUS, programa do Governo Federal instituído pela Portaria GM/MS nº 1.434 de 28 de maio de 2020, que visa a integração das informações de saúde dos cidadãos em uma grande rede de dados (BRASIL, 2020a), como forma de instrumentalizar a Estratégia Brasileira de Saúde Digital². O programa permitiu o desenvolvimento do aplicativo Conecte Sus Cidadão que possibilita ao usuário o acesso a sua carteira de vacinação digital, certificado nacional de vacinação de COVID-19, resultados de exames laboratoriais de COVID-19, registros de doações de sangue e acompanhamento da posição na fila de transplante. A referida portaria designou também a criação da Rede Nacional de Dados em Saúde para interoperabilidade e integração de

¹Destaca-se que, existem alguns estudiosos que preferem adotar o entendimento de que o dado e a informação não são expressões sinônimas, mas sim estágios diferentes do mesmo fenômeno. O dado seria uma a informação em potencial, isto é, ainda não tratada. Entretanto, é bastante comum que a doutrina e a legislação as utilizem com o mesmo significado.

² A Estratégia Brasileira de Saúde Digital é a aplicação nacional da Estratégia Global de Saúde Digital elaborada pela Organização Mundial da Saúde (OMS) visando o emprego de tecnologias de informação e comunicação na construção de soluções para o sistema de saúde.

informações referentes a atenção, vigilância e gestão à saúde. O projeto piloto do RNDS estava focada no Estado de Alagoas, visto que o Estado possuía apenas 214 UBS informatizadas das 947 em funcionamento no seu território (BRASIL, 2019a). Mas em decorrência da calamidade pública causada pela pandemia do coronavírus, o projeto foi redirecionado para recepção e integração de notificações e resultados de exames laboratoriais relacionados à doença e disseminação dos resultados dos exames aos cidadãos e profissionais de saúde. Inclusive, de acordo com o Ministério da Saúde (BRASIL, 2021a), entre março e novembro de 2020, a Rede recebeu em torno de 4 milhões de resultados de exames de COVID-19. Relevante citar, ainda, que integra a RNDS, o Cadastro Nacional de Pessoas para Saúde (BRASIL, 2017a), que deve conter informações que possibilitem a identificação unívoca da pessoa como dados de identificação, endereçamento e domicílio, de contato com a pessoa ou familiares, filiação e informações sociodemográficas. Esse sistema digital vinculará os diversos registros de informações de saúde sobre a pessoa para possibilitar a recuperação do seu histórico de saúde e disponibilizar estatísticas sociodemográficas para tomadas de decisões em saúde.

Do mesmo modo, a Administração faz uso o Cadastro Nacional de Informações Sociais para gerir principalmente os dados previdenciários, trabalhistas e sociais do brasileiro, necessários para a concessão de benefícios previdenciários, por exemplo. O extrato proveniente desse cadastro fornece, além de informações identificadoras, os vínculos de trabalho que a pessoa teve ao longo da vida e a remuneração que recebia, bem como detalhes sobre os benefícios que já requereu ou recebeu. Aliás, é por esse motivo que o Decreto nº 3.048, responsável por regulamentar o Regime Geral da Previdência Social, dispõe no art. 19 que esse extrato (comumente chamado de CNIS) é apto provar à filiação a previdência social, tempo de contribuição e salário de contribuição.

O Cadastro Único para Programas Sociais do Governo Federal funciona na mesma lógica com relação a assistência social, uma vez que manuseia dados capazes de identificar e caracterizar famílias de baixa renda. A qualificação desses grupos familiares é exigida para sua seleção e integração em programas sociais, tais como o Programa Bolsa Família ou Minha Casa Minha Vida. A esse respeito, é importante apontar que pelo menos 25 projetos sociais federais exigem como condição o cadastramento da pessoa ou da família nesse sistema (BRASIL, 2019b). Para isso, são coletadas informações acerca das características do domicílio de uma família, total de seus membros e despesas mensais, rendimentos, escolaridade, situação no mercado de trabalho, além dos dados cadastrais como o nome, documento de identificação e endereço (BRASIL, 2019c). Outro aspecto notável do CadÚnico é o Cadastramento Diferenciado, estabelecido no art. 24 da

Portaria MDS nº 177 de 16 de junho de 2011, que reúne informações sobre famílias pertencentes a Grupos Populacionais Tradicionais e Específicos como famílias indígenas, quilombolas, ciganas e pertencentes a comunidades de terreiro (BRASIL, 2019d).

Todos esses cadastros e projetos descritos mostraram-se imprescindíveis ao Estado brasileiro durante a crise sanitária vivida nos anos de 2020 e 2021 resultante da pandemia do covid-19. O Conecte Sus, por exemplo, agrupou um grande conjunto de informações relativas a óbitos e infecções pelo coronavírus, que foram manuseados para compreender o comportamento da doença no país e definir estratégias de enfrentamento. Além disso, considerando o agravamento das dificuldades econômicas da população, muitas famílias se socorreram dos programas de assistência social para sobreviver nesse período³.

Diante do exposto, foi possível demonstrar em pequena escala a importância dos dados pessoais da população brasileira na execução de serviços atinentes a Seguridade Social. O tratamento desses dados, portanto, se revela mais do que necessário para a garantia de direitos sociais previstos na Constituição Federal, bem como na concretização dos fundamentos e objetivos do próprio Estado brasileiro.

2.2 As implicações do tratamento de dados pessoais no direito à privacidade

A utilização de dados pessoais para o incremento da qualidade e eficiência de processos produtivos, produtos e serviços se tornou imprescindível na realidade atual. Isso se dá, em grande medida pela evolução das tecnologias da informação (BEZERRA SALLES SARLET; MOLINARO, 2020, p.184), com consequente aumento da capacidade de armazenamento de dados por um valor não mais tão alto e a produção de novos conhecimentos a partir da aplicação de técnicas para encontrar padrões e ligações entre dados que aparentemente não possuíam qualquer relação.

Por conseguinte, foram sendo construídas novas relações sociais, econômicas e políticas em torno da multiplicidade de dados disponíveis não só sobre fenômenos como também pessoas ou comunidades e a possibilidade de sua transformação em um ativo através da aplicação de tecnologias da informação (DONEDA, 2019, p. 137).

Essas alterações na realidade social exigiram que categorias tradicionais do direito fosse repensadas para que pudessem atender as novas demandas. É o caso do direito à privacidade, cuja construção num primeiro momento se deu a partir de uma perspectiva patrimonialista, enquanto signo diferenciador de uma classe social que buscava atingir os ideais liberais e individualistas (RODOTÁ, 2008, p. 26-270). A sua proteção foi concebida

³De acordo com os dados verificados através da ferramenta CECAD, disponibilizada pelo Ministério da Cidadania, o número de famílias beneficiárias do Programa Bolsa Família em março de 2022 ultrapassou em, pelo menos, 1 milhão a quantidade verificada no mesmo mês do ano anterior.

então como uma reafirmação da identidade da burguesia e assumia o papel de garantir que o indivíduo pudesse tratar de assuntos da sua esfera privada sem a intromissão de terceiros estranhos. Era uma tutela direcionada o direito de ser deixado só, que teve bastante influência do pensamento jurídico norte-americano, especialmente com a publicação do artigo *"The Right to Privacy"* de Samuel Dennis Warren e Louis Dembitz Brandeis em 1890.

Essa perspectiva, contudo, foi se mostrando insuficiente diante da crescente possibilidade técnica do Estado de coletar e armazenar informações sobre seus cidadãos. Em outras palavras:

A ampliação do conceito de privacy se deu, em grande medida, por conta da evolução das formas de divulgação e apreensão de dados pessoais. Com o advento de novas tecnologias, notadamente o desenvolvimento da biotecnologia e da Internet, o acesso a dados sensíveis e, conseqüentemente, a sua divulgação, foram facilitados de forma extrema. (MULHOLLAND, 2019, p. 172)

Diante desse cenário, constatou-se que a proteção da privacidade restrita apenas a proteção da propriedade de um indivíduo não era mais suficiente, já que ela era um aspecto essencial da realização da pessoa enquanto ser humano dotado de valores e ideais pessoais, os quais pode ou não escolher tornar público (MORI, 2011, p.34). Em outras palavras, a proteção da privacidade implicaria não só na proteção da liberdade do indivíduo, como também a garantia de que possa desenvolver sua personalidade sem temer que esse processo seja catalogado e utilizado sem o seu consentimento. O que também era necessário para proteger e sustentar o sistema democrático, na medida em que permite que o sujeito interprete a realidade conforme suas experiências e valores pessoais sem medo de sanções de caráter moral, social ou institucional decorrentes da constante vigilância (RODOTÁ, 2011, p. 129), o que permite o desenvolvimento de um diálogo saudável com a coletividade para garantir a consecução do seu melhor interesse. Nesse sentido, Danilo Doneda (2019, p. 128-129) destaca que:

A privacidade assume, portanto, posição de destaque na proteção da pessoa humana, não somente tomada como um escudo contra o exterior – na lógica da exclusão - mas como elemento indutor da autonomia, da cidadania, da própria atividade política em sentido amplo e dos direitos de liberdade de uma forma geral. Nesse papel, ela é pressuposto de uma sociedade democrática moderna, da qual o dissenso e o anticonformismo são componentes orgânicos.

É nesse ponto que o direito da privacidade se relaciona a tutela dos dados pessoais, mas com ela não se confunde (2011, p. 91-108). Como já mencionado anteriormente,

todos os aspectos da vida hoje estão intimamente relacionados com o uso de produtos que coletam dados constantemente. Desde celulares, a computadores pessoais ou até geladeiras inteligentes, há uma vasta quantidade de tecnologias que permitem a coleta diária de uma imensidão de informações sobre a vida privada da população pelo mundo. Desse modo, pode-se falar que existe no ambiente virtual uma verdadeira representação da personalidade do indivíduo, tendo em vista que quase todos os seus aspectos podem ser encontrados em bancos de dados (LIMBERGER, 2007, p. 58). Assim, a noção de privacidade não mais comporta limites fixos de propriedade e a sua violação se tornou muito mais simples, já que a maior parte das informações concernentes a vida privada, ou até a intimidade de alguém, podem ser obtidas através de dados que não foram necessariamente coletados para esse fim, mas que quando conjugados por uma determinada lógica fornecem um “raio x” da pessoa. É por esse motivo, inclusive, que os dados sensíveis ganham especial atenção nos ordenamentos jurídicos pelo mundo. As informações que esses dados carregam não só expõe caracteres muito íntimos da personalidade de uma pessoa, como também impedem o seu desenvolvimento em situação de igualdade com os demais (2007, p. 62). Ou seja, o tratamento de dados pessoais sensíveis apresenta riscos que vão além da violação apenas da privacidade, podendo atingir uma dimensão maior da própria dignidade da pessoa humana, porque impede que ela seja tratada com igualdade.

Como consequência da observação dessas circunstâncias, ocorreu um movimento para a regulamentação do direito a proteção de dados pessoais, como um direito autônomo, separado da proteção da privacidade que já tinha previsão na Constituição Federal e no Código Civil. Em 14 de agosto de 2018 foi publicada a Lei nº 13.709, chamada de Lei Geral de Proteção de Dados, com o objetivo de estabelecer regras e diretrizes para o tratamento de dados pessoais no país⁴. A legislação foi fortemente influenciada pelo modelo europeu, em grande parte consubstanciado no Regulamento Geral de Proteção de Dados (GDPR) instituído pela União Europeia e em vigor desde maio de 2018. A normativa europeia enfoca o consentimento do titular dos dados pessoais com base na autodeterminação informativa⁵, bem como na atuação proativa dos agentes de tratamento em uma lógica muito mais preventiva do que reativa. Em suma, pode-se dizer que:

[...] o regulamento Europeu propõe o dever de atuação positiva do responsável pelo tratamento de dados, de modo que ele adote medidas técnicas e organizativas de acordo com a (i) natureza dos dados protegidos,

⁴Um ponto digno de nota é que, embora a regulamentação da proteção de direitos pessoais seja bem recente, o Código de Defesa do Consumidor já trazia regras específicas para tutelar os dados dos consumidores.

(ii) o contexto tecnológico que circunda o tratamento daqueles e (iii) o grau de risco de violação a direitos e liberdades fundamentais. (ENGERLMANN; SZINVELSKI, 2020, p. 99)

Acompanhando essa orientação, a LGPD definiu como fundamento da proteção de dados pessoais, entre outros, a autodeterminação informativa e estabeleceu como requisito para o tratamento de dados o consentimento. Além disso, estipulou uma série de direitos ao titular dos dados pessoais que serão tratados e deveres aos agentes desse tratamento, de modo a resguardar a sua privacidade e garantir uma resposta proporcional e adequada quando da sua violação.

Destaca-se, ainda, que dispensou um regime diferenciado aos dados pessoais categorizados como sensíveis em observância ao princípio da não discriminação e da finalidade, levando em consideração o já mencionado potencial discriminatório que carregam. Um exemplo, é o condicionamento do seu tratamento ao consentimento específico e destacado do titular, que não será exigido apenas em hipóteses que em sua maioria envolvam o interesse da coletividade, previstos no art. 11 da lei.

2.3 Os efeitos das falhas na proteção de dados pessoais no âmbito da Seguridade Social no mundo jurídico

Fixadas as premissas acerca da importância do uso de dados pessoais pela Administração Pública quando da execução de serviços ligados à Seguridade Social e do risco a privacidade dos administrados que esse tratamento gera, cumpre examinar como o Poder Público tem lidado com falhas na proteção dos dados pessoais sob sua tutela.

Para isso, foram selecionadas situações amplamente divulgadas pela imprensa de vazamento de dados pessoais pelos órgãos ou entidades responsáveis pela execução dos serviços de saúde, previdência e assistência social. Considerando os eventos escolhidos, o outro passo foi buscar quais foram as medidas tomadas pelas instituições envolvidas e se chegou a existir provocação do Judiciário pelos prejudicados.

Levando em consideração o já comentado projeto do Ministério da Saúde para implementar a Estratégia Brasileira de Saúde Digital, durante a pandemia a pasta fez uso de vários sistemas informáticos para gerenciar a sua atuação no manejo da doença no país. Dois desses sistemas foram acidentalmente expostos por um funcionário do Hospital Albert Einstein, que estaria trabalhando em conjunto com o Ministério da Saúde em um projeto focado em estratégias para análise de *big data*, expondo os dados de ao menos 16 milhões de brasileiros com suspeita ou confirmação de COVID-19 (CAMBRICOLI, 2020). De acordo com o jornal Estado de São Paulo, o responsável pelo acidente teria deixado expostas credenciais que davam acesso aos sistemas E-SUS-VE e Sivep-Gripe,

que traziam informações como CPF, endereço, telefone e doenças pré-existentes de pessoas que apresentavam quadro confirmado de covid-19 ou suspeita. Diante do ocorrido, o deputado Alexandre Padilha do PT/SP, por meio do Requerimento de Informação nº 1548/2020 na Câmara dos Deputados, pediu informações ao Ministro da Saúde acerca das medidas de proteção aos dados pessoais de sua responsabilidade e sobre o próprio vazamento. Em resposta, a Secretaria de Vigilância em Saúde informou que o Hospital Albert Einstein notificou o Ministério Público da correção da divulgação accidental pelo cientista de dados por ele contratado e que não tinham sido encontradas evidências de vazamento de dados. A seu turno, o Departamento de Informática do Sistema Único de Saúde indicou que foram feitos ajustes para evitar que acontecimentos semelhantes se repetissem.

Acontece que, um mês depois, veio à tona outra falha na segurança do sistema de e-SUS-Notifica que deixou aberto a consulta os dados de pelos 243 milhões de brasileiros, número superior ao da população na época porque incluía informações de pessoas já falecidas. Dessa vez, as credenciais ficaram expostas no código do site e poderiam ser facilmente acessadas por qualquer usuário através da função “inspecionar elemento” nos navegadores da Internet. Sobre o ocorrido o Ministério da Saúde apenas comentou que as falhas estavam sendo corrigidas e novas medidas de prevenção estavam sendo tomadas, bem como que já havia iniciado a apuração do incidente.

Interessante mencionar que a Open Knowledge Brasil já havia notificado o Ministério da Saúde em junho de 2020 a respeito de um problema semelhante. De acordo com ong, o sistema e-SUS VE/Notifica além de expor informações pessoais e médicas de pessoas com suspeita de covid, ainda deixava exposto no próprio código do sistema, credenciais que davam acesso a um repositório de relatórios exportados por usuários autorizados.

Considerando esses acontecimentos, o Ministério Público Federal, na sede do Inquérito Civil nº 1.34.001.008528/2020-35, instaurado para apurar responsabilidades sobre as irregularidades na proteção de dados pessoais sensíveis constantes nos bancos de dados do Sistema Único de Saúde e a consequente exposição indevida, elaborou a Recomendação GAB-LLO nº 25/2021. De acordo com a Recomendação, restou constatado que falha responsável por deixar acessível os dados de 243 milhões de brasileiros “evidencia que o monitoramento da segurança, feito pelo Ministério da Saúde, sobre o acesso e funcionamento de seus bancos de dados é insuficiente, o que põe em risco a privacidade e a intimidade de milhões de cidadãos brasileiros.”. Assim sendo, recomendou que órgão adotasse uma série de medidas como a produção ou publicização do Relatório de Impacto à Proteção de Dados Pessoais, em conformidade com o art. 5º,

XII da LGPD, e a informação quanto a adequação do tratamento de dados pessoais sensíveis as normas técnicas de segurança da informação e proteção da privacidade.

Quase seis meses depois, já no final de 2021, o sistema do Ministério da Saúde sofreu um ataque hacker, assumido pelo grupo “Lapsus\$ Group”, que alterou a aparência do site saúde.gov para expor mensagem anunciando que os dados internos do sistema haviam sido copiados e excluídos. Por conta disso, a Polícia Federal informou em nota que teria iniciado investigação para apurar a materialidade e autoria da conduta. Na mesma linha, o Ministério Público, no Inquérito Civil já mencionado, requereu ao Ministério da Saúde que prestasse informações sobre o ataque externo

Apesar desse último caso não se tratar propriamente de vazamento de dados pessoais, mas sim de sequestro de dados, o acontecimento demonstra a fragilidade da segurança dos dados pessoais armazenados nos bancos de dados do Ministério da Saúde, principalmente considerando a série de ocorrências anteriores. Mesmo assim, parece que ainda não existem ações nem de tutela coletiva nem individual para responsabilização pelas falhas ocorridas e a violação da privacidade e da proteção de dados pessoais delas decorrentes.

O que não é o caso quando se trata do vazamento de dados pessoais no âmbito do Instituto Nacional de Seguro Social. Atualmente, já existem pelo menos quatro ações civis públicas⁶ tramitando no Tribunal Regional Federal objetivando a condenação do INSS pela violação dos dados pessoais dos segurados do Regime Geral da Previdência Social. Duas delas foram propostas pelo Ministério Público Federal não só contra a autarquia federal, como também contra as empresas fizeram uso dos dados vazados.

Uma dessas ações foi julgada parcialmente⁷ procedente em maio de 2019 para condenar o INSS a obrigação de implementar medidas administrativas para evitar a violação de dados pessoais sob sua tutela e incidentes de segurança, bem como a tomar medidas necessárias para responsabilizar civil e administrativamente servidores e terceiros responsáveis pela violação. No caso em questão, o Ministério Público Federal teria apurado em Inquérito Civil que vários segurados estavam recebendo propagandas dos serviços da empresa Tifim Recuperadora de Créditos e Cobranças Ltda – Me, mesmo antes de serem notificados do deferimento dos seus pedidos de benefício previdenciário. Embora não tenha restado comprovado que a empresa estaria obtendo esses dados

⁶ Trata-se das ações de nº 0017291-65.2016.4.03.6100, proposta perante 2ª Vara Cível Federal de São Paulo, nº 101289144.2019.4.01.3803 que tramita perante 3ª Vara Federal Cível e Criminal da SSJ de Uberlândia-MG, nº 104118984.2021.4.01.3800 e nº 080107729.2021.4.05.8300 que estão sendo processadas na 12ª Vara Federal de Pernambuco.

⁷ Trata-se da Ação Civil Pública nº 0017291-65.2016.4.03.610 que tramita na 2ª Vara Cível Federal de São Paulo e foi julgada em 20/05/2019.

pessoais de forma ilícita, o juízo da 2ª Vara Cível Federal de São Paulo entendeu suficientemente provado que o INSS não estaria dando a devida proteção aos dados dos segurados do regime geral da previdência social. Entretanto, não houve condenação do réu no pagamento de indenização por danos individuais ou coletivos, visto que faltaram provas quanto a existência de prejuízo.

Com argumentos bastante semelhantes, o Ministério Público Federal também propôs ação civil pública em face do INSS e da empresa Perfecta Intermediações de Negócios Eireli, que ainda está pendente de julgamento.

As outras duas ações foram propostas por organizações da sociedade civil, tomando como argumento não só a proteção de dados pessoais, como também a proteção do consumidor frente as propagandas abusivas das instituições financeiras. Tanto o Instituto de Defesa Coletiva quanto o Instituto Brasileiro De Política e Direito da Informática entraram com a ação contra o INSS e o Dataprev, empresa responsável por..., em função do repasse não autorizado pelo titular de seus dados pessoais as instituições financeiras, que por vezes se aproveitam dessa ferramenta para praticar marketing abusivo. Assim como o caso anterior, essas causas ainda não foram julgadas.

Levanto em contra essa breve análise de casos de vazamento de dados pessoais no âmbito da Seguridade Social, é possível inferir que existe a necessidade de adequação das entidades e órgãos desse setor aos preceitos da Lei Geral de Proteção de Dados, especialmente no que tange a privacidade. Isto porque, como já mencionado, a Administração Pública realiza o tratamento de uma ampla gama de dados pessoais para que consiga prestar os serviços atinentes a saúde, assistência e previdência social. Aliás, muitos desses dados são categorizados como sensíveis, o que exigirá das instituições uma infraestrutura de segurança maior e mais complexa. Além disso, é preciso enfatizar que em razão dessa quantidade expressiva de dados tratados, o Poder Público tem em mãos uma verdadeira representação virtual da personalidade da população brasileira. Isso pode se apresentar como um risco constante de violação dessa personalidade, caso não sejam adotadas as medidas necessárias de segurança para evitar o uso inadequado desses dados.

3. CONSIDERAÇÕES FINAIS

Diante do desenvolvido até aqui, não resta dúvidas sobre a relevância que os dados pessoais têm para a sociedade atual. Eles se tornaram uma engrenagem essencial no funcionamento da vida humana porque é com a informação que as tecnologias fornecem soluções eficazes para tornar o dia a dia mais cômodo.

Por isso, parece instintivo concluir que o Estado, que precisa fornecer uma quantidade expressiva de serviços para consecução do interesse público, também precisa fazer uso dos dados pessoais. É a partir do tratamento das informações fornecidas pela população brasileira que torna-se possível desenvolver estratégias para responder as necessidades da coletividade.

Nesse ponto, o tratamento de dados pessoais pela Seguridade Social é indispensável. São as instituições pertencentes a esse sistema que agem diretamente na promoção de direitos essenciais para o desenvolvimento socioeconômico do país, tendo em vista que abrangem a saúde, assistência e previdência social. Para que o Poder Público possa salvaguardar esses direitos a todos, é necessário a prestação mais eficaz e eficiente das atribuições conferidas pela lei e pela Constituição Federal aos entes e entidades responsáveis pela manutenção da Seguridade Social. Em grande medida as tecnologias da informação a partir do tratamento de dados oferecem um considerável incremento na eficiência e eficácia na prestação dos serviços públicos.

No entanto, considerando que os dados pessoais são extensões da personalidade do indivíduo, a Administração Pública precisa estar preparada para assegurar a segurança na sua manipulação. E mais, nas áreas de saúde, previdência e assistência os dados coletados trazem uma variedade de informações muito específicas e até íntimas sobre a pessoa, de modo que o cuidado precisa ser redobrado quando da sua proteção, inclusive para resguardar a sua privacidade.

Apesar disso, ao que parece a Administração Pública tem apresentado certa dificuldade para implementar a estrutura necessária para garantir a proteção dos dados pessoais sob sua responsabilidade nos termos da Lei Geral de Proteção de Dados. Conforme foi examinado no presente estudo, há indícios de que os sistemas informatizados dos órgãos e entidades responsável pela prestação dos serviços de saúde e previdência não foram capazes de prevenir falhas de segurança e vazamentos de dados.

Por outro lado, é digno de nota que essas falhas não passaram despercebidas. Tanto que não só o Ministério Público deu início a investigações para apurar os vazamento de dados pelo Ministério da Saúde e propôs ação civil pública para responsabilizar o Instituto Nacional de Seguridade Social por esse motivo, como também a sociedade civil, por meio de organizações sem fins lucrativos, buscou o Poder Judiciário para obter resposta justa aos danos decorrentes da violação dos dados pessoais de segurados do Regime Geral da Previdência Social.

Diante dessas considerações, é possível concluir que existe a necessidade de readequação da estrutura informática das instituições abrangidas pela Seguridade Social

a Lei Geral de Proteção de Dados e às normas referentes a proteção da privacidade e a segurança da informação. Além disso, observar-se que há um movimento, ainda que tímido, no ordenamento jurídico brasileiro para responder as demandas geradas pelas novas relações criadas pela rápida evolução das tecnologias da informação.

4. REFERÊNCIAS

AGÊNCIA SENADO. Comissão discute vazamento de dados do INSS para empréstimos consignados. 06 jun. 2019. Disponível em: <<https://www12.senado.leg.br/noticias/audios/2019/06/comissao-discute-vazamento-de-dados-do-inss-para-emprestimos-consignados>> Acesso em: 06 fev. 2021

ALMEIDA, Bethania de Araujo et al. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. *Ciência & Saúde Coletiva* [online]. 2020, v. 25, suppl 1 [Acessado 12 Junho 2022] , p. 2487-2492. Disponível em: <<https://doi.org/10.1590/1413-81232020256.1.11792020>>. Epub 05 Jun 2020. ISSN 1678-4561. <https://doi.org/10.1590/1413-81232020256.1.11792020>.

BALERA, Wagner. *A Seguridade Social na Constituição de 1988*. São Paulo: Editora Revista dos Tribunais, 1989

BALERA, Wagner. *Sistema de Seguridade Social*. 4. ed. São Paulo: LTr, 2006.

BEZERRA SALES SARLET, G.; MOLINARO, C. A. Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de big data. *Revista Brasileira de Direitos Fundamentais & Justiça*, [S. l.], v. 13, n. 41, p. 183–212, 2020. DOI: 10.30899/dfj.v13i41.811. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/811>. Acesso em: 12 jun. 2022.

BOSCHETTI, Ivanete. *Seguridade social no Brasil: conquistas e limites à sua efetivação*. In: *Serviço Social: direitos sociais e competências profissionais*. Brasília: CFESS/ABEPSS, 2009.

BRASIL. Constituição Federal (1988). *Constituição Federativa do Brasil*, de 5 outubro de 1988 Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em: 07 fev. 2021.

BRASIL. Lei nº 10.406, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Brasília, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 jun. 2022.

BRASIL. Ministério da Saúde. Portaria de Consolidação nº 1. *Diário Oficial da União*, Brasília, DF, 28 set de 2017. Disponível em: <https://bvsms.saude.gov.br/bvs/saudelegis/gm/2017/prc0001_03_10_2017.html>. Acesso em: 28 nov. 2021.

CAMBRICOLI, Fabiana. Vazamento de senha do Ministério da Saúde expõe dados de 16 milhões de pacientes de covid. *O Estado de S. Paulo*. 26 nov. 2020. Disponível em: <https://saude.estadao.com.br/noticias/geral,vazamento-de-senha-do-ministerio-da-saude-expoe-dados-de-16-milhoes-de-pacientes-de-covid,70003528583>. Acesso em: 13 jun. 2022.

CASTELANI, Clayton; BRIGATTI, Fernanda. Aposentados sofrem assédio para contratar consignado. Agora São Paulo. 20 abr. 2015. Disponível em: <https://agora.folha.uol.com.br/grana/2015/04/1618693-aposentados-sofrem-assedio-para-contratar-consignado.shtml>. Acesso em: 13 jun. 2022.

CORREIA, Marcus Orione Golçalves; CORREIA, Érica Paula Barcha. Curso de Seguridade Social. 2. ed. São Paulo: Saraiva, 2002.

COSTA, José Augusto Fontoura. Tratamento de dados de saúde: limites ao compartilhamento de dados sensíveis. In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos Monaco. LGPD na Saúde. São Paulo: Thomas Reuters, 2021. 89-102

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law [EJL], [S. l.], v. 12, n. 2, p. 91–108, 2011. Disponível em: <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315>. Acesso em: 12 jun. 2022.

DONEDA, Danilo. Privacidade e Informação. Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados. São Paulo: Thomson Reuters, 2019.

DRESCH, Rafael de Freitas Valle; SILVA, Renan Boccacio Souza da. Breves apontamentos sobre a autodeterminação informativa e o direito fundamental à proteção de dados. In: GHILARDI, Dóris; SASS, Liz Beatriz (coord.). Temas Atuais de Direito Privado e Sociedade da Informação: o direito na era digital. 1. ed. Florianópolis: Habitus, 2020. cap. 6, p. 115-123.

ENGELMANN, Wilson; SZINVELSKI, Mártin M. Risco Cibernético no Tratamento de Dados Pessoais e Autodeterminação Informativa: Reflexões à Luz da Lei Geral de Proteção de Dados (Lei N.º 13.709/2018). In: GHILARDI, Dóris; SASS, Liz Beatriz (coord.). Temas Atuais de Direito Privado e Sociedade da Informação: o direito na era digital. 1. ed. Florianópolis: Habitus, 2020. cap. 5, p. 95-114.

FLEURY, S. Reforma do estado, seguridade social e saúde no Brasil. In: MATTA, GC., and LIMA, JCF. orgs. Estado, sociedade e formação profissional em saúde: contradições e desafios em 20 anos de SUS [online]. Rio de Janeiro: Editora FIOCRUZ, 2008, pp. 49-87.

FLEURY, Sonia. A seguridade social inconclusa. Disponível <<http://app.ebape.fgv.br/comum/arq/Seguridade.pdf>>. Acesso 05/2022

Lazzari, João Batista; CASTRO, Carlos Alberto Pereira de. Capítulo 2: A Seguridade Social no Brasil. In: Direito Previdenciário. 2 ed. Rio de Janeiro: Forense-Método, 2021

LIMBERGER, Têmis. O Direito à Intimidade na Era da Informação: A necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado Editora, 2007.

LOTT, Yuri Monnerat; CIANCONI, Regina de Barros. Vigilância e privacidade, no contexto do Big Data e dados pessoais: análise da produção da Ciência da Informação no Brasil. Perspectivas em Ciência da Informação, [S.l.], v. 23, n. 4, p. 117-132, dez. 2018. ISSN 19815344. Disponível em: <<http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/3313>>. Acesso em: 12 jun. 2022.

MAGRANI, Eduardo. Entre dados e robôs: Ética e privacidade na era da hiperconectividade. 2. ed. Porto Alegre: Arquipélago Editorial, 2019.

MINISTÉRIO DA CIDADANIA. Cadastro Único. 2019. Disponível em: <<https://www.gov.br/cidadania/pt-br/acoes-e-programas/cadastro-unico/o-que-e-e-para-que-serve-1>>. Acesso em: 28 nov. 2021.

MINISTÉRIO DA CIDADANIA.. Cadastro Único - Dados. 2019. Disponível em: <<https://www.gov.br/cidadania/pt-br/acoes-e-programas/cadastro-unico/dados>>. Acesso em: 28 nov. 2021.

MINISTÉRIO DA CIDADANIA. Cadastramento Diferenciado. 2019. Disponível em: <<https://www.gov.br/cidadania/pt-br/acoes-e-programas/servicos/cadastro-unico/gestao-do-cadastro-unico-1/processo-de-cadastramento/cadastramento-diferenciado>>. Acesso em: 28 nov. 2021.

MINISTÉRIO DA CIDADANIA. Cecad 2.0. Disponível em: <<https://cecad.cidadania.gov.br/painel04.php>> Acesso: 12 jun. 2016.

MINISTÉRIO DA SAÚDE. Apresentação da Reunião Técnica RNDS – Lançamento em Alagoas 12.11.2019. <<https://www.gov.br/saude/pt-br/assuntos/saude-digital/material-de-apoio/ApresentaodaReunioTcnicaRNDSLanamentoemAlagoas12.11.2019.pdf>> Disponível em: <https://bvsms.saude.gov.br/bvs/saudelegis/gm/2017/prc0001_03_10_2017.html>. Acesso em: 16 jun. 2022.

MINISTÉRIO DA SAÚDE. O Programa Conecte SUS. Disponível em: <<https://www.gov.br/saude/pt-br/assuntos/saude-digital/o-programa-conecte-sus/o-programa-conecte-sus>>. Acesso em: 28 nov. 2021.

MINISTÉRIO DA SAÚDE. Rede Nacional de Dados em Saúde - RNDS. Disponível em: <<https://www.gov.br/saude/pt-br/assuntos/rnds>>. Acesso em: 28 nov. 2021.

MIRANDA, Victor Vasconcelos. O direito à privacidade na era digital e as tutelas assecuratórias. Fórum de Direito Civil - RFDC, Belo Horizonte, ano 5, ed. 12, 2016.

MORI, Michele Keiko. Direito à intimidade versus informática. Curitiba: Juruá, 2001.

MULHOLLAND, C. S. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). Revista de Direitos e Garantias Fundamentais, v. 19, n. 3, p. 159-180, 29 dez. 2018.

PALHARES, GABRIELA CAPOBIANCO et al. A privacidade em tempos de pandemia e a escada de monitoramento e rastreio. Estudos Avançados [online]. 2020, v. 34, n. 99 [Acessado 12 Junho 2022] , pp. 175-190. Disponível em: <<https://doi.org/10.1590/s0103-4014.2020.3499.011>>.

PILATI, José Isaac; OLIVO, Mikhail Vieira Cancelier de. Direito à privacidade: uma nova perspectiva. Revista Novos Estudos Jurídicos, [s. l.], v. 19, n. 1, 4 jan. 2014.

POLÍCIA FEDERAL, Coordenação-Geral de Comunicação Social. Atuação da PF no ataque hacker ao Ministério da Saúde. 10 dez. 2021. Disponível em: <https://www.gov.br/pf/pt-br/assuntos/noticias/2021/12/atuacao-da-pf-no-ataque-hacker-ao-ministerio-da-saude>. Acesso em: 13 jun. 2022.

PROCURADORIA DA REPÚBLICA NO DISTRITO FEDERAL. 2º Ofício de Atos Administrativos, Consumidor e Ordem Econômica. Requerimento GAB-LLO nº 25/2021. Brasília, 24 set. 2021.

ROVER, Aires José. Direitos humanos e proteção dos dados pessoais em tempos de inteligência artificial: uma bibliometria temática. In: GHILARDI, Dóris; SASS, Liz Beatriz (coord.). Temas Atuais de Direito Privado e Sociedade da Informação: o direito na era digital. 1. ed. cap. 4, p. 79-94.

SILVA, Luciana Vasco da. A Lei geral de proteção de dados e suas implicações a seguradoras e operadoras de plano de saúde. Porto Alegre, Revista brasileira de direito comercial, v. 6, n. 32, p. 108–119, dez./jan., 2019.

TAPAJÓS, Luiza Maria. Seguridade social: aportes tecnológicos como elemento de democratização e controle social. Seguridade, assistência social e cidadania, Florianópolis, n. 4, p. 53-63, 1 jan. 1999.

VENTURA, Miriam; COELI, Cláudia Medina. Para além da privacidade: direito à informação na saúde, proteção de dados pessoais e governança. Cadernos de Saúde Pública, [s. l.], ano 7, n. 34, 23 jul. 2018.

VENTURINI, Jamila. Da privacidade à transparência: desafios da interação entre agentes públicos e privados na gestão de informações pessoais. Revista Eletrônica de Comunicação Informação & Inovação em Saúde, [s. l.], v. 10, ed. 4, 22 dez. 2016.

Contatos: anammoraes03@outlook.com e ana.scalquette@mackenzie.br