Universidade do Minho
Escola de Direito

Nivaldo Cortês Bonifácio

A aplicação da lei de proteção de dados no âmbito dos Tribunais de Contas

Outubro de 2020

A aplicação da lei geral de proteção de dados no âmbito dos Tribunais de Contas
Nivaldo Cortês Bonifácio
UMinho | 2020

Universidade do Minho
Escola de Direito

Nivaldo Cortês Bonifácio

A aplicação da lei geral de proteção de dados no âmbito dos Tribunais de Contas

Dissertação de Mestrado

Mestrado em Direito e Informática

Trabalho realizado sob a orientação dos Professores Doutores

Teresa Coelho Moreira

Paulo Novais

Outubro de 2020

Direitos de autor e condições de utilização do trabalho por terceiros

Este é um trabalho académico que pode ser utilizado por terceiros desde que respeitadas as regras e boas práticas internacionalmente aceites, no que concerne aos direitos de autor e direitos conexos.

Assim, o presente trabalho pode ser utilizado nos termos previstos na licença abaixo indicada.

Caso o utilizador necessite de permissão para poder fazer um uso do trabalho em condições não previstas no licenciamento indicado, deverá contactar o autor, através do RepositóriUM da Universidade do Minho.

Licença concedida aos utilizadores deste trabalho

Atribuição CC BY

https://creativecommons.org/licenses/by/4.0/

Universidade do Minho, Braga, de de 2020.

Nivaldo Cortês Bonifácio

AGRADECIMENTOS

A Deus, por estar sempre presente em minha vida e cuja luz está a guiar-me e dar-me a sabedoria para enfrentar os desafios que se apresentam na caminhada pessoal e profissional.

A minha esposa Ana, que sempre esteve a meu lado, incentivando-me nas escolhas e, sobretudo, sacrificando o seu precioso tempo para apoiar-me e motivar-me, quer durante a elaboração da presente dissertação, quer ao longo de toda a minha vida profissional, académica e pessoal.

A meus pais, hoje representado por minha mãe, Leda, a eterna gratidão a qual não é o suficiente para expressar o que sinto em relação a eles.

Aos meus orientadores, a Senhora Professora Doutora Teresa Alexandra Coelho Moreira e o Senhor Professor Doutor Paulo Novais, pela disponibilidade de tempo, de conhecimento e inestimável ajuda, sem os quais não teria sido possível a concretização deste projeto.

Ao Tribunal de Contas de Portugal, em especial ao Juiz Conselheiro José F. F. Tavares e ao Dr. Antônio Melo pela acolhida e colaboração essenciais para o alcance dos objetivos propostos no presente trabalho.

Ao Tribunal de Contas do Estado do Rio Grande do Norte, em especial aos amigos Conselheiro Gilberto Jales e Conselheiro Poti, por meio dos quais agradeço aos demais Conselheiros.

Ao Tribunal de Contas do Estado da Paraíba, em especial ao amigo e incentivador Conselheiro Arthur Paredes da Cunha Lima; ao Conselheiro e Presidente da ATRICON Fábio Túlio Filgueira Nogueira, por meio de quem agradeço aos demais pares que constroem a cada dia um TCE/PB mais atuante e eficiente.

Aos colegas do Tribunal de Contas: Rutênio, Vinicius, André, Diego – TCE/RN; ao meu amigo Diretor Geral, Dr. Humberto Porto; e aos demais parceiros de trabalho Ed Wilson, Humberto Gurgel, Josedilton – TCE/PB; pela preciosa e valorosa contribuição.

DECLARAÇÃO DE INTEGRIDADE

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ou resultados em nenhuma das etapas conducente à sua elaboração.

Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

Universidade do Minho, Braga, de de 2020.

Nivaldo Cortês Bonifácio

RESUMO

Ao longo da história o mundo tem se curvado às evoluções tecnológicas, as quais se incorporam na sociedade trazendo inovações no estilo de vida das pessoas, instituições públicas e privadas, corporações etc. A comunicação se tornou mais imediata, o acesso às informações e dados ocorrem instantaneamente, na medida em que o trânsito de dados na Internet torna-se, a cada incremento nas novas tecnologias de informação e comunicação - NTIC, acessível a todos nas mais variadas formas, plataformas e ferramentas disponíveis, expondo a público a vida dos cidadãos indiscriminadamente. Tendo em conta este desenvolvimento exponencial da tecnologia da informação, os legisladores, têm se dedicado a fundo na elaboração de normas que visem regulamentar o uso dos dados e informações que transitam pela rede mundial de computadores, visando a proteção do usuário e a garantia da preservação da sua privacidade. Entre os diplomas legais atinentes a esta temática sobressai-se o Regulamento Geral sobre Proteção de Dados - RGPD da Europa, no qual inspirou-se a Lei Geral de Proteção de Dados Pessoais - LGPD do Brasil, os quais trazem regras a serem observadas pelas Entidades Governamentais, nas quais se incluem o TCE/RN, o TCE/PB, a exemplo do que vem ocorrendo com o Tribunal de Contas de Portugal. É neste contexto que o presente estudo faz uma análise da aplicação das regras de proteção de dados nas atividades destas Entidades Constitucionais, o que envolve a adequação de suas normas interna corporis aos requisitos e princípios das legislações protetivas de dados pessoais; os sitemas de gestão de TI disponíveis; a integração com algumas legislações correlatas, e.g. da Lei de Acesso à Informação; a averiguação do nível do conhecimento que os funcionários destes organismos públicos têm acerca da LGPD e do RGPD; entre outras questões atinentes ao tema proposto. Requer-se, portanto, uma aplicação de forma integrada das leis, conciliando-as, de tal modo que sejam respeitados os direitos assegurados aos titulares dos dados, sem olvidar, contudo que, diante de um tema tão atual e inovador, existem muitos pontos obscuros que deverão pautar as discussões durante e também após a implementação das regras de conformidade no setor público. Isto exige a adoção de uma postura mais proativa não apenas das Entidades pesquisadas, porquanto, tal como o que tem ocorrido nos países europeus, em virtude da implantação do RGPD, a administração pública tem andado a passos lentos quando se trata de adequação à LGPD.

Palavras-chave: LGPD; RGPD; Regras; Requisitos; Aplicação; Tribunais de Contas.

ABSTRACT

Throughout history the world has been bending to technological developments, which are incorporated into society, bringing innovations in the lifestyle of people, public and private institutions, corporations etc. Communication has become more immediate, access to information and data occurs instantly as data traffic on the Internet becomes, with each increment in new information and communication technologies – NICT, accessible to all in the most varied forms, platforms and tools available, exposing citizens' lives to the public indiscriminately. Taking into account this exponential development of information technology, legislators have been deeply dedicated to the development of rules that aim to regulate the use of data and information that travel through the world wide web, aiming at protecting the user and ensuring the preservation of their privacy. Among the legal diplomas pertaining to this theme, the General Regulation on Data Protection - GDPR of Europe stands out, which inspired the General Law on Protection of Personal Data - LGPD do Brasil, which bring rules to be observed by the Governmental Entities, which include the TCE / RN, the TCE / PB, as is the case with the Court of Auditors of Portugal. It is in this context that the present study analyzes the application of data protection rules in the activities of these Constitutional Entities, which involves adapting their internal corporate rules to the requirements and principles of personal data protection laws; the available IT management systems; integration with some related legislation, e.g. the Access to Information Law; the verification of the level of knowledge that the employees of these public bodies have about the LGPD and the GDPR; among other issues related to the proposed theme. Therefore, an integrated application of the laws is required, reconciling them, in such a way that the rights assured to data subjects are respected, without forgetting, however, that in the face of such a current and innovative theme, there are many obscure points that should guide the discussions during and also after the implementation of compliance rules in the public sector. This requires the adoption of a more proactive stance, not only of the Entities surveyed, because, like what has happened in European countries, due to the implementation of the GDPR, the public administration has been moving at a slow pace when it comes to adaptation to the LGPD.

Keywords: LGPD; GDPR; Rules; Requirements; Application; Courts of Accounts.

ÍNDICE

ABREVIATURAS E SIGLAS

AIPD – Avaliação de Impacto sobre a Proteção de Dados

ANPD - Autoridade Nacional de Proteção de Dados

Apud.- Citado por

AR – Assembleia da República

Art. – Artigo

ASTEC – Assessotia Técnica do Tribunal de Contas

CC – Código Civil

CDC – Código de Defesa do Consumidor

CDFUE – Carta dos Direitos Fundamentais da União Europeia

CE – Conselho da Europa

Cfe. - Conforme

CNPD – Comissão Nacional de Proteção de Dados

CRFB – Constituição da República Federativa do Brasil

CRP – Constituição da República Portuguesa

CCTCI - Comissão de Ciência, Tecnologia, Comunicação e Informática

DGTC – Direção Geral do Tribunal de Contas

DSTI - Departamento de Sistemas e Tecnologias de Informação

EDPB - Comité Europeu para a Proteção de Dados

EPD – Encarregado de Proteção de Dados

ESATC - Estatuto dos Serviços de Apoio do Tribunal de Contas

e.g. do latim exempli gratia, «por exemplo»

GENT - Sistema de Gestão de Entidades, do Tribunal de Contas de Portugal

LAI - Lei de Acesso à Informação – Lei n° 12.527/2011, de 18 de dezembro de 2011.

LCE – Lei Complementar Estadual

LGPD – Lei n° 13.853/2019, de 8 de julho de 2019, que alterou a Lei n° 13.709/2018, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais

LINDB - Lei de Introdução as Normas de Direito Brasileiro

MCTIC - Ministério da Ciência, Tecnologia, Comunicação e Informática

MP – Medida Provisória

MPDFT – Ministério Público do Distrito Federal e Territórios

MPOG – Ministério do Planejamento, Orçamento e Gestão

NTIC - Novas Tecnologias de Informação e Comunicação

Op. cit. – Obra citada

p. – Página

PG. – Plenário Geral do TC. de Portugal

PL – Projeto de Lei

RGPD – Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016 - Regulamento Geral sobre Proteção de Dados

RN-TC – Resolução Normativa do Tribunal de Contas

SIAI Fiscal - Sistema Integrado de Auditoria Informatizada, do TCE/RN

SAGRES - Sistema de Acompanhamento da Gestão dos Recursos da Sociedade, do TCE/PB

TCE/PB – Tibunal de Contas do Estado da Paraíba

TCE/RN – Tribunal de Contas do Estado do Rio Grande do Norte

TC. de Portugal – Tribunal de Contas de Portugal

TC's – Tribunais de Contas

TCU – Tribunal de Contas da União

TFUE – Tratado sobre o Funcionamento da União Europeia

TI – Tecnologia da Informação

TJUE - Tribunal de Justiça da União Europeia

TUE – Tratado da União Europeia

UE - União Europeia.

INTRODUÇÃO

"Todos têm a ideia central de resguardar o cidadão contra o uso abusivo e indiscriminado dos seus dados pessoais"[1]. Inicia-se o presente trabalho fazendo-se alusão à citação em epígrafe, não por acaso, mas propriamente por ser factível que ao longo da história o mundo tem se curvado às evoluções tecnológicas, as quais se incorporam na sociedade trazendo inovações no estilo de vida das pessoas, instituições públicas e privadas, corporações etc.

Observa-se que, nas duas últimas décadas, a comunicação se tornou mais imediata, o acesso às informações e dados ocorrem instantaneamente, na medida em que o trânsito de dados na Internet torna-se, a cada incremento nas novas tecnologias de informação e comunicação - NTIC, acessível a todos nas mais variadas formas, plataformas e ferramentas disponíveis, dispositivos eletrónicos, *e.g.* das redes sociais *online,* telemóveis sofisticados*,* enfim, no dizer de Teresa Moreira um "admirável mundo novo"[2], que expõe a público a vida dos cidadãos indiscriminadamente.

Tendo em conta este desenvolvimento exponencial da tecnologia da informação, as autoridades governamentais, notadamente os legisladores, têm se dedicado a fundo na elaboração de normas que visem regulamentar o uso dos dados e informações que transitam pela rede mundial de computadores, visando a proteção do usuário e a garantia da preservação da sua privacidade. Os diplomas legais atinentes a esta temática não se limitam à iniciativa privada, vale dizer, trazem regras a serem observadas pelas Entidades Governamentais em todos os níveis.

A par destas iniciativas legislativas, e seguindo o modelo do RGPD, os demais países têm se dedicado à regulamentação da proteção de dados em seus territórios, a exemplo do Brasil que, em 8 julho de 2019, teve sancionada a Lei 13.853/2019, que alterou a LGPD (Lei 13.709/2018). A referida norma legislativa, além de flexibilizar alguns pontos, ensejou a criação da Autoridade Nacional de Proteção de Dados (ANPD) para fiscalizar o seu cumprimento, iniciativa esta que gerou muitas críticas em sua composição por parte dos estudiosos da matéria, e para a qual dever-se-á reservar espaço no conteúdo deste trabalho. Dado que o âmbito de aplicação da supra referida LGPD abrange também as Entidades Públicas, conforme consta do Art. 1°, do Capítulo I[3], e traz no Capítulo IV regras específicas

---

[1] TOFFOLI, José Antonio Dias - na abertura do *"Seminário sobre a Lei Geral de Proteção de Dados: a caminho da efetividade"*, realizado no Superior Tribunal de Justiça - STJ em parceria com outros órgãos e entidades - *Julho, 2019*. Disponível em: <https://stj.jusbrasil.com.br/noticias>. Acessado em: 10 de dez. de 2019.

[2] MOREIRA, Teresa Coelho. "*As Novas Tecnologias de Informação e Comunicação: um Adminirável Mundo Novo no Trabalho", in Revista de Direito e Garantias Fundamentais,* Vitória, n° 11, 2012, p.15-52.

[3] Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acessado em: 10 de dez. de 2019.

a serem observadas pelo Poder Público no tratamento de dados pessoais, fez-se necessária a adequação de suas normas *interna corporis* à LGPD por parte dos Órgãos Administrativos.

Este trabalho de incorporação das regras da LGPD aos respectivos âmbitos dos Órgãos e Entidades que compõem a Administração Pública, especificamente no Brasil, vem sendo desenvolvido paulatinamente e espera-se que até a entrada em vigor da retromencionada lei, notadamente em meados de 2020, esteja concluído, respeitando-se, contudo, as limitações Institucionais, a exemplo da disponibilidade de recursos orçamentários necessários à sua concretização.

Neste contexto, inserem-se os Tribunais de Contas do Brasil, bem como o Tribunal de Contas de Portugal, posto que devem adotar procedimentos internos com vistas ao tratamento de dados, tanto em relação aos seus servidores quanto em relação à recolha e armazenamento de dados pessoais de seus jurisdicionados, mormente no sentido de evitar vazamentos e acesso indevido por pessoas não autorizadas, que é um dos grandes desafios e embates a serem enfrentados na atualidade. Ademais, conforme atesta Teresa Moreira, "para além da recolha de dados, há uma possibilidade sempre presente de retenção, recomposição e descontextualização dos dados recolhidos"[4].

A alimentação de dados abertos e informações prestadas pelos jurisdicionados e demais pessoas aos TC's, e o consequente armazenamento em seu banco de dados, facilitados pelo uso da *Internet*, que é uma rede aberta, permite, concomitantemente, a respectiva comunicação e difusão dessas informações, a partilha e muitas outras funções. Por outro lado, exige a criação ou o aperfeiçoamento de mecanismos e ferramentas de controle que visem dar um mínimo de proteção a esses dados, o que deve ser feito e guiado em harmonização com as garantias dos direitos fundamentais Constitucionais e demais legislações infraconstitucionais, a exemplo da Lei n° 26, de 22 de agosto de 2016[5], de Portugal, e da Lei n° 12.527, de 18 de dezembro de 2011, a denominada Lei de Acesso à Informação – LAI, do Brasil.

Torna-se, portanto, imprescindível realizar uma pesquisa no campo objeto do Tema deste trabalho, intitulado "a aplicação da lei geral de proteção de dados no âmbito dos Tribunais de Contas", a fim de obter respostas quanto à aplicação da referida Lei e quais ferramentas dispõem alguns Tribunais de Contas para fazer face às regras atinentes ao tratamento de dados pessoais, sem que incorram em infração às garantias aos direitos fundamentais assegurados ao cidadão pela Constituição e legislações correlatas. Desta forma, ter-se-á por base para elementos de investigação o TCE/RN, o Tribunal de

---

[4] MOREIRA, Teresa Coelho. "*A Privacidade dos trabalhadores e as Novas Tecnologias de Informação e Comunicação: Contributo para um Estudo dos Limites do Poder de Controlo Electrónico do Empregador, Coimbra, Almedina, 2010, p.55.*.

[5] Aprova o regime de acesso à informação administrativa e ambiental e de reutilização dos documentos administrativos, transpondo a Diretiva 2003/4/CE, do Parlamento Europeu e do Conselho, de 28 de janeiro, e a Diretiva 2003/98/CE, do Parlamento Europeu e do Conselho, de 17 de novembro. Disponível em: <www.dre.pt/pesquisa>. Acessado em: 12 de dez. de 2019.

TCE/PB, ambos do Brasil, e o TC. de Portugal. Em relação a este último, em cuja estrutura se insere as Secções Regionais dos Açores e da Madeira, a abordagem limitar-se-á ao Tribunal de Contas – Sede, localizado em Lisboa.

Contudo, no intuito de melhor se compreender a temática proposta, cujo objetivo traduz-se na análise do nível de implantação do RGPD e da LGPD no âmbito das Entidades Públicas referenciadas alhures, necessário se faz contextualizá-la de forma distinta, posto que o RGPD encontra-se praticamente assimilado pelos Estados-Membros, não se podendo afirmar neste sentido em relação à LGPD. Destarte, a despeito de relevantes discussões, debates, audiências, reuniões do gênero por instituições e associações representativas da sociedade brasileira em torno da aprovação de uma legislaçào de proteção de dados pessoais, optou-se por abordar os principais pontos debatidos no Seminário de Proteção de Dados Pessoais realizado no Brasil pela Comissão de Tecnologia, Comunicação e Informática e a Comissão Especial do PL 4.060/12, em 22 de Maio de 2018, os quais foram, pela sua abrangência, essenciais na decisão de se levar a cabo a elaboração da LGPD no País. Finalizando a primeira parte do tema, serão abordados alguns conceitos gerais ou termos que têm passado a fazer parte do quotidiano das áreas da tecnologia da informação das Entidades Públicas, além de outros intimamente relacionados com a LGPD e o RGPD.

No segundo capítulo, será abordado o âmbito de aplicação material do RGPD, bem como o tratamento de dados pessoais aos órgãos ou agências da UE, além das regras específicas do Poder Público no Brasil aplicáveis ao tratamento de dados pessoais. Interessa, pois, precipuamente, ao escopo deste trabalho, as disposições legais do Capítulo IV da LGPD do Brasil e as correlatas do RGPD europeu, os quais se referem ao tratamento de dados pessoais pelo Poder Público. Não apenas dos dados que digam respeito aos próprios servidores, mas, também, os dados que são alimentados pelos jurisdicionados e demais pessoas e entidades que devam legalmente prestar informações ao Poder Público e, em particular, aos TC's de Portugal e dos Estados da Paraíba e do Rio Grande do Norte, estes dois últimos do território brasileiro. Em decorrência dessas regras, é imperativo dedicar-se algumas linhas abordando um aparente conflito entre duas legislações, quais sejam, a que garante o direito de acesso à informação e a que resguarda a proteção de dados pessoais.

Uma vez analisadas estas questões, passar-se-á ao estudo da aplicação das regras de proteção de dados pelas três Entidades da Administração Pública objeto de pesquisa, quais sejam o TCE/RN, o TCE/PB e o TC. de Portugal. Esta parte está dividida em dois capítulos: o capítulo III, o qual apresenta o resultado e análise de pesquisa de campo na três Entidades Públicas, produto da observação e estudo dos atos normativos existentes *in loco* sobre o tema, bem como de um questionário realizado por amostra com os servidores/funcionários públicos desses Tribunais de Contas; e o capítulo IV, o qual apresenta os

sistemas de acompanhamento de gestão utilizados por cada um dos TC's e respectivas ferramentas de proteção de dados. Paralelamente a isto, e considerando o objetivo a que se propõe alcançar, buscar-se-á apresentar exemplos de materialização das regras trazidas nas leis de proteção de dados (RGPD e LGPD) aplicadas ou a serem desenvolvidas nas três Entidades Públicas pesquisadas, do ponto de vista da área de informática. A propósito de tal ênfase neste aspecto, não posso prescindir de contribuir com a minha opinião, no sentido de apresentar alternativas a serem seguidas pelos respectivos setores de informática com vistas a melhor adequação às regras da RGPD e LGPD.

Esta será, no essencial, a estrutura adotada para a presente dissertação de mestrado, ao final da qual se pretende responder especificamente a algumas questões, fruto da análise acerca do confronto entre as legislações sobre proteção de dados pessoais e a legislação de acesso à informação; da investigação, sobre a perspectiva legal, do âmbito material de aplicação do RGPD e LGPD pelos citados Tribunais de Contas; verificar como os TC's têm se dedicado na implementação das regras de proteção de dados nas suas atividades. Por fim, far-se-á algumas considerações expondo de forma crítica a nossa opinião sobre o tema, bem como possíveis sugestões a serem seguidas para aperfeiçoar as questões relacionadas à escorreita aplicação das legislações sobre proteção de dados pessoais no âmbito dos referenciados Tribunais Contas.

CAPÍTULO I – Contextualização, precedentes e conceitos principais

1.1. Breve Contextualização do Tema

Como afirmado no introito deste trabalho, é inegável a importância das tecnologias da informação no quotidiano da sociedade moderna, notadamente com a evolução alcançada nos últimos 30 (trinta) anos, alimentada pelo acesso generalizado à *Internet*. O que, em princípio, parecia um canal alternativo para o acesso a informação, o entretenimento, a socialização etc, tornou-se uma verdadeira virtualização da sociedade, gerando, em consequência, a recolha, o transporte e o armazenamento de um volume de dados jamais imaginado.

É cediço, porém, que as capacidades tecnológicas de recolha e armazenamento de dados avançaram a passos muito mais largos do que capacidade humana de processamento, o que reflete sobremaneira nas entidades com acesso a fontes contínuas de informacão, sejam estas leituras de consumos de luz, água, gás, ou outros meios de acesso de que se valem os usuários ou operadores de TI. Entretanto, a certeza que se tem acerca da informação como um bem a ser protegido, preservado e valorado determina que o seu armazenamento seja feito, embora não se tenha uma ideia clara de que utilização lhe pode ser dada.

Tal constatação, ameaça sobremaneira o direito à intimidade e à vida privada do indivíduo, os quais estão intimamente ligados à personalidade. Trata-se do direito que cada pessoa tem a poder decidir por si só o quê (e quando) deve ser partilhado com terceiras pessoas, permitindo ao indivíduo o controlo da sua própria vida e experiências, nas esferas em que não é permitida uma intromissão, nem por parte do Estado nem por parte de terceiras pessoas[6]. Este é um direito intimamente ligado à liberdade pessoal, à construção da identidade, ao controlo que cada um deve ter sobre os aspectos da identidade que deseja projetar para o mundo[7]. No Ordenamento Jurídico Português, este direito à privacidade aparece expressamente reconhecido e consagrado pelos artigos 26º nº 1 da CRP e 70º do CCP (entendido como

---

[6] Nas palavras de Catarina Sarmento e Castro, p. 22-28, cfe. Janeiro, D.B. "*La protección de datos de carácter personal en el derecho comunitario"*. In *"Estudos de Direito da Comunicação*", Instituto Jurídico da Comunicação, Faculdade de Direito, Universidade de Coimbra, 2002, que, a págs. 44 e nota 37 refere a existência de direitos fundamentais de terceira geração. Apud ANDRADE, Francisco C.P.; COSTA, Angelo; NOVAIS, Paulo. *Privacidade e Proteção de Dados nos cuidados de saúde de idosos*. UMINHO. Artigo em ata de conferência. 2011. p. 12. Disponível em: <http://repositorium.sdum.uminho.pt/handle/1822/15197>. Acessado em: 01 de julho de 2020.

[7] Segundo Rouvroy, A., "*Privacy Data Protection and the Unprecedented Challenges of Ambient Intelligence*". In: "Studies in Ethics, Law and Technology", 2008, v. 2 (1), p. 8. 18 -- Cfe. Rouvroy, idem, pág 9. Apud ANDRADE, Francisco C.P.; COSTA, Angelo; NOVAIS, Paulo. *Privacidade e Proteção de Dados nos cuidados de saúde de idosos*. UMINHO. Artigo em ata de conferência. 2011. p. 12. Disponível em: <http://repositorium.sdum.uminho.pt/handle/1822/15197> Acessado em: 01 de julho de 2020.

um direito de personalidade)[8]. Há de ser respeitado este direito e limitada a interferência e o acesso por qualquer meio à comunicação de cunho pessoal, não podendo nem mesmo "[...] o empregador invocar os seus legítimos poderes de organização, direção e controlo para limitar o exercício do direito constitucional [...]" assegurado ao trabalhador, no dizer de Teresa Moreira[9]. Por outro lado, torna-se necessário estabelecer um equilíbrio entre a tutela destes direitos e o respeito às regras legitimamente impostas pelo empregador, eis que o trabalhador ou mesmo o funcionário público terão a faculdade de usufruir "[...] de tempo pessoal, inclusive de caráter muito privado, durante o trabalho".[10]

A despeito de tal preocupação, verifica-se a existência de grandes benefícios para a utilização da informação recolhida, a exemplo de publicação de estatísticas oficiais, a associação de dados através de *data mining* (mineração de dados) em diversas áreas, em especial registros médicos, ou ainda, como uma forma de melhorar a experiência dos utilizadores, aperfeiçoando resultados de pesquisas online etc. Tais benefícios, contudo, defrontam-se com restrições impostas pela obrigatoriedade de proteger a privacidade de terceiros, o que faz emergir um problema de recorrente questionamento, qual seja, como publicar informação referente a pessoas, de forma a obter diversos benefícios e, concomitantemente, proteger a sua privacidade?

Eis a batalha a ser enfrentada, apresentar ou fornecer uma solução para dirimir o conflito de interesses surgido entre os que detêm a informação e a pretendem valorizar e aqueles a quem a informação diz respeito de forma que não lhes seja comprometida a privacidade. Trata-se, pois, de equacionar o aparente conflito entre o direito de acesso à informação e o direito fundamental de proteção do indivíduo em sua integridade e universalidade.

Neste contexto, e tendo em vista a edição do RGPD, já em vigor, bem como a recente publicação da LGPD do Brasil, a entrar em vigência em agosto de 2020, muito se tem debatido sobre a escorreita aplicação destes diplomas legais por profissionais da área jurídica, sejam eles doutrinadores, magistrados, operadores do direito etc.

A incorporação das regras de proteção de dados pessoais definidas no RGPD e na LGPD aplica-se igualmente às instituições, órgãos, organismos ou agências estatais no âmbito das respectivas esferas de governo (em toda a União Europeia e, em se tratando do Brasil, à União, Estados e Municípios).

---

[8] ANDRADE, Francisco C.P.; COSTA, Angelo; NOVAIS, Paulo. *Privacidade e Proteção de Dados nos cuidados de saúde de idosos*. UMINHO. Artigo em ata de conferência. 2011. p. 12. Disponível em: <http://repositorium.sdum.uminho.pt/handle/1822/15197>. Acesso em: 01 de julho de 2020.

[9] MOREIRA, Teresa Coelho. "*A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação: contributo para um estudo dos limites do controlo eletrónico do empregador, Almedina, 2010., p.* 424.

[10] Ibid. p.787.

Os Órgãos que compõem a Administração Pública e, especificamente no presente estudo, os TC's do Brasil, bem como o TC. de Portugal, revestem-se, como referenciado alhures, de responsabilidade ímpar no tratamento de dados, tanto em relação aos seus servidores quanto em relação à recolha e armazenamento de dados pessoais de seus jurisdicionados, mormente no sentido de evitar vazamentos e acesso indevido por pessoas não autorizadas, que é um dos grandes desafios e embates a serem enfrentados na atualidade.

Ademais, como já explicitado, a ameaça à privacidade, as violações de direitos pelas empresas que tratam dados e formam *Big Data*[11] *e Data Lake*[12], conhecem perfis, atuam com ofertas diferenciadas para os seus clientes, discriminam e conhecem o comportamento de cada usuário têm sido objeto de análise e de pesquisa tanto no meio acadêmico quanto por parte do Estado, notadamente pelo fato de ter entre as suas atribuições constitucionais o dever de promover o desenvolvimento econômico, tecnológico e a inovação.[13]

---

[11] No contexto de uma sociedade de vigilância, o *Big Data* tudo vê, sendo capaz de capturar todas as pegadas digitais dos usuários para, a partir daí, utilizar seus "poderes" não apenas para registrar e processar o passado e o presente, como também para antecipar e decidir o futuro das pessoas. E o mais preocupante é que faz tudo isso sem a devida transparência e *accountability*, já que os algoritmos utilizados por governos e grandes agentes empresariais são normalmente considerados segredos, respectivamente de Estado ou de negócios. Disponível em: <https://www.academia.edu/40236159/Responsabilidade_civil_de_administradores_de_sociedades_empres%C3%A1rias_por_decis%C3%B5es_tomadas_com_base_em_sistemas_de_intelig%C3%AAncia_artificial>. Acessado em: 02 de jun. de 2020.

[12] Um *Data Lake* (lago de dados), por exemplo, possibilita que grandes volumes de dados estruturados e não estruturados sejam armazenados de forma flexível e elástica em formatos próximos aos de origem. O objetivo de um lago de dados é apresentar uma visão não refinada das informações para ajudar os profissionais que com eles trabalham a explorar técnicas de análise de dados, independentemente das restrições que possam existir em um armazém de dados tradicional. Disponível em: <www.serpro.gov.br/menu/noticias-2017/data-lake-e-big-data-sao-tendencia-no-uso-de-dados-publicos>. Acesso em: 02 de jun. de 2020.

[13] Acerca desta desta afirmação, o Art. 218 da Constituição da República Federativa do Brasil dispõe, com clareza, nos termos seguintes: Art. 218. O Estado promoverá e incentivará o desenvolvimento científico, a pesquisa, a capacitação científica e tecnológica e a inovação.

§ 1º A pesquisa científica básica e tecnológica receberá tratamento prioritário do Estado, tendo em vista o bem público e o progresso da ciência, tecnologia e inovação.

§ 2º A pesquisa tecnológica voltar-se-á preponderantemente para a solução dos problemas brasileiros e para o desenvolvimento do sistema produtivo nacional e regional.

§ 3º O Estado apoiará a formação de recursos humanos nas áreas de ciência, pesquisa, tecnologia e inovação, inclusive por meio do apoio às atividades de extensão tecnológica, e concederá aos que delas se ocupem meios e condições especiais de trabalho.

§ 4º A lei apoiará e estimulará as empresas que invistam em pesquisa, criação de tecnologia adequada ao País, formação e aperfeiçoamento de seus recursos humanos e que pratiquem sistemas de remuneração que assegurem ao empregado, desvinculada do salário, participação nos ganhos econômicos resultantes da produtividade de seu trabalho.

§ 5º É facultado aos Estados e ao Distrito Federal vincular parcela de sua receita orçamentária a entidades públicas de fomento ao ensino e à pesquisa científica e tecnológica.

§ 6º O Estado, na execução das atividades previstas no caput, estimulará a articulação entre entes, tanto públicos quanto privados, nas diversas esferas de governo.

De outra banda, o tema privacidade é alvo de discussão que remonta ao século passado e já não era sem tempo que as instituições, órgãos, organismos ou agências estatais no âmbito das respectivas esferas de governo também esboçassem preocupação e se alinhassem a este processo. Este interesse com a proteção dos dados das pessoas vem acentuando-se ao longo dos anos junto à sociedade bem como tem exigido uma postura ativa dos Poderes Legislativos Europeu e Brasileiro, sendo que, no caso do Brasil, passou a ter maior destaque, notadamente, quando da aprovação do Marco Civil da Internet, instituído pela Lei n° 12.965, de 23 de abril de 2014.

Paralelamente a esse fato foram as discussões levada a cabo no âmbito de doutrinadores e legisladores no Brasil, as quais culminaram com propostas de emendas de suma importância, a exemplo da questão da tutela dos dados pessoais e da responsabilidade dos agentes de tratamento, como também a cristalização de importantes conceitos, tais como a necessidade de obtenção de consentimento para o tratamento de dados sensíveis e a definição clara dos procedimentos que devem pautar a interconexão de dados entre responsáveis. Neste norte, amadureceu-se a idéia de não permitir o compartilhamento de dados pessoais com terceiros sem o consentimento "livre, inequívoco, informado, expresso e específico" do titular. Ademais, os debates acarretaram como consequência, no âmbito do referido Marco Civil da Internet, uma extensa, precisa e objetiva definição do que constituem dados pessoais.

É de se destacar o importante trabalho desenvolvido pela comissão legislativa especial destinada a proferir parecer ao projeto de Lei nº 4060, de 2012 que dispôs sobre o tratamento e proteção de dados pessoais[14], o qual deu o arcabouço à Lei nº 13.709, de 14 de agosto de 2018, alterada pela lei nº 13.853, de 8 de julho de 2019, ambas dispondo sobre a proteção de dados pessoais, sendo esta última a criar a Autoridade Nacional de Proteção de Dados - ANPD, no caso do Brasil.

Ressalte-se que as propostas apresentadas no âmbito das discussões realizadas no Brasil, estão inseridas em um contexto mundial, sobrepondo-se às legislações nacionais e delas exigindo o tratamento da questão dos dados pessoais e proteção das pessoas de forma harmônica. Frise-se, ainda, o fato de que a construção de um arcabouço similar entre os países traz como consequência a criação de um ambiente propício aos negócios, precipuamente globais, oriundos do manuseio de dados.

No contexto do TC. de Portugal, verifica-se que o ano de 2019 trouxe importantes decisões na área da privacidade, tanto por parte da Assembleia da República, mediante a aprovação de importantes

---

§ 7º O Estado promoverá e incentivará a atuação no exterior das instituições públicas de ciência, tecnologia e inovação, com vistas à execução das atividades previstas no caput. Disponível em: <www.planalto.gov.br>. Acessado em: 17 de jan. de 2020.

[14] Projeto de Lei (PL) nº 4.060, de 2012, de autoria do Deputado Milton Monti, dispondo sobre o tratamento de dados pessoais. Apensos à proposição principal encontram-se os PLs 5.276/16, do Poder Executivo, e 6.291/16, do Dep. João Derly. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=>. Acessado em: 17 de jan. de 2020.

leis, quanto de Pareceres e deliberações emitidas pela CNPD e pelo EDPB, além de Acórdãos do TJUE, os quais repercutiram também no âmbito da Administração Pública e, por conseguinte, no TC. de Portugal, notadamente em virtude do precedente encaminhamento da Proposta de Lei n° 126/XIII à AR, sobre a qual tecer-se-á comentário no decorrer deste trabalho.

A AR aprovou as seguintes leis: Lei n° 58/2019[15], de 8 de agosto de 2019, a qual assegura a execução do RGPD na ordem jurídica nacional, RGPD; a Lei n.º 59/2019[16], de 8 de agosto de 2109, que aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680[17] do Parlamento Europeu e do Conselho, de 27 de abril de 2016; e a Lei n.º 46/2019[18], de 8 de julho de 2019, que altera o regime do exercício da atividade de segurança privada e da autoproteção, que consistiu na primeira alteração à Lei n.º 34/2013, de 16 de maio de 2013.

A atuação do EDPB refletiu-se em importantes diretrizes[19], entre as quais destacaram-se: parecer sobre a base legal para o tratamento de dados pessoais no contexto de ensaios clínicos, designadamente no que respeita ao uso primário de dados para o próprio protocolo dos ensaios clínicos e ao uso secundário para outros fins científicos; deliberação sobre a interação entre a Diretiva *ePrivacy*[20] e o RGPD, no sentido de que aquela norma (e respectivas leis de transposição) *é lex specialis*, o que significa que a "norma especial" relativa ao tratamento de dados pessoais terá precedência sobre o RGPD; publicação, para consulta pública, da versão prévia das diretrizes relativas ao tratamento de dados pessoais através de sistemas de videovigilância; estabeleceu-se a versão final das diretrizes sobre o âmbito de aplicação da alínea b), do n° 1. do artigo 6° do RGPD[21] no contexto dos serviços da

---

[15] Disponível em: <https://eur-lex.europa.eu/homepage.html?locale=pt>. Acessado em: 20 de Nov. de 2019.

[16] Ibid.

[17] A Diretiva relativa à proteção dos dados destinados às autoridades policiais e judiciárias faz parte do pacote de reformas da proteção de dados da UE, juntamente com o Regulamento Geral sobre a Proteção de Dados - Regulamento (UE) 2016/679, e visa proteger os dados pessoais das pessoas singulares quando são tratados pelas autoridades policiais e judiciárias bem como melhorar a cooperação no combate ao terrorismo e à criminalidade transfronteiras na União Europeia (UE) permitindo às autoridades policiais e judiciárias dos países da UE trocarem informações necessárias para que as investigações sejam mais eficazes e mais eficientes. Disponível em: <https://eur-lex.europa.eu/homepage.html?locale=pt>. Acesso em: 20 de Nov. de 2019.

[18] Disponível em: <https://eur-lex.europa.eu/homepage.html?locale=pt > . Acessado em: 20 de Nov. de 2019.

[19] Disponível em: <https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_pt>. Acessado em: 20 de Nov. de 2019

[20] Diretiva *ePrivacy*, que estabelece as regras que regem o tratamento de dados pessoais e a abordagem da privacidade no sector das comunicações eletrónicas.disponível em: <www.anacom.pt>. Acessado em: 20 de Nov. de 2019.

[21] ARTIGO 6°

Licitude do Tratamento

O Tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:

sociedade de informação, sendo abordados os fundamentos legais para o tratamento de dados para execução de um contrato no qual o titular dos dados é parte ou para a realização de diligências pré-contratuais, nomeadamente no âmbito da publicidade comportamental.

O EDPB definiu, ainda em 2019, a versão final das diretrizes relativas ao âmbito territorial de aplicação do RGPD, as quais visam fornecer uma interpretação comum aos vários Estados-Membros para avaliarem se uma determinada atividade de tratamento se enquadra no âmbito de aplicação territorial do RGPD, além de publicar, para consulta pública, a Diretriz 4/2019 sobre a proteção de dados desde a concepção e por defeito, e das diretrizes sobre os critérios do Direito ao Esquecimento nos casos de motores de busca no âmbito do RGPD. Ademais, aprovou as listas dos tratamentos de dados pessoais sujeitos à AIPD, nos termos do n.º 4 do Artigo 35.º do RGPD[22].

A seu turno, a CNPD, por meio da Deliberação 2019/494[23], entendeu por desaplicar algumas normas da Lei n.º 58/2019, de 8 de agosto, sob a alegação de que estas contradizem manifestamente o estatuído no RGPD e, pela Deliberação 2019/495[24], que versa sobre a dispensa de aplicação de coimas às entidades públicas, prevista no n.º 2 do artigo 44.º e no artigo 59.º da Lei 58/2019, de 8 de agosto, considerou que só é possível requerer tal dispensa fundamentada após acusação da prática de um ilícito contraordenacional. A CNPD estabeleceu, entre as suas diretrizes[25], a Diretriz 1/2019, relativa ao tratamento de dados pessoais no contexto de campanhas eleitorais e marketing político, e a Diretriz 2/2019, concernente ao tratamento de dados pessoais no contexto das redes inteligentes de distribuição

---

b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados. Disponível em: <https://eur-lex.europa.eu/homepage.html?locale=pt>. Acessado em 21 de Nov.de 2019.

[22] *RGPD: Diretrizes, recomendações e melhores práticas.* Disponível em: <https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_pt>. Acessado em: 21 de Nov.de 2019.

[23] A CNPD considerou que algumas normas da Lei n° 58/2019 não podem sequer ser salvas por uma «interpretação corretiva» conforme ao direito da UE, «por ser insuprível a antinomia com as normas do RGPD e com a Carta dos Direitos Fundamentais da União Europeia», pelo que a CNPD violaria o RGPD se aplicasse a lei nacional. A deliberação da CNPD fundamenta-se na Constituição Portuguesa, que preceitua no seu artigo 8.º que as disposições dos Tratados e as normas emanadas das instituições da UE são aplicáveis na ordem jurídica interna nos termos definidos pelo direito da União, e na jurisprudência do Tribunal de Justiça da UE que determina que as entidades administrativas estão obrigadas a desaplicar as normas nacionais que contrariem o direito da UE. Consequentemente, a CNPD decidiu fixar as normas da lei nacional que, sendo manifestamente incompatíveis com o direito da União, exigem a adoção de tal deliberação, e que desaplicará em casos futuros que venha a apreciar. Disponível em: <https://www.cnpd.pt/home/relacoes/comunicados/desaplicacao_normas_lei_58_2019.pdf>. Acessado em: 21 de Nov.de 2019.

[24] Sobre esta temática, a CNPD vem por meio da Deliberação 2019/495 esclarecer que "interpreta o disposto no n.º2 do artigo 44.º da Lei n.º 58/2019 no sentido de este lhe conferir um poder discricionário de apreciar, apenas no caso concreto de verificação prática de um facto ilícito em violação do disposto no RGPD ou naquela lei, se se justifica afastar a regra legal de aplicação de uma sanção pecuniária (coima) a um determinado organismo público, enquanto responsável pelo tratamento (ou subcontratante), tendo em consta os diferentes interesses e direitos em presença). Disponível em: <https://www.cnpd.pt/bin/decisoes/Delib/DEL_2019_495.pdf)->, Acessado em 22 de Nov.de 2019.

[25] Decisões da CNPD. Disponível em: < https://www.cnpd.pt/home/decisoes/diretrizes/diretrizes.htm>. Acesso em: 22 de Nov. de 2019.

de energia elétrica.

Importantes Acórdãos[26] proferidos em 2019 pelo TJUE hão de ser observados pelas Entidades Públicas, ainda que indiretamente, entre os quais podem ser citados: o Acórdão *Fashion ID* (C-40/17), segundo o qual os operadores de sites são responsáveis conjuntos com o *Facebook* pelo tratamento de dados recolhidos e a ele transmitidos por meio de um *plug-in like*[27], que permite ao *Facebook* recolher dados pessoais do *site* do operador; o Acórdão *Planet49* (C-673/17)[28], por meio do qual confirma-se que a declaração de consentimento através de uma opção pré-validada não é válida como consentimento para o uso de *cookies*, devendo o responsável pelo tratamento fornecer ao utilizador informações sobre os *cookies*, tais como a duração do tratamento e a permissão ou não do acesso por terceiros; o Acordão *Google* (Direito ao Esquecimento) (C-136/17), o qual explicita que ao se aceitar um pedido de exercício de um direito ao esquecimento, o operador de um motor de busca não tem de efetuar o apagamento dos resultados em todas as versões do seu motor, devendo fazê-lo apenas nas versões correspondentes aos Estados-Membros (*URLs*). Por fim, cabe ressaltar o parecer da advocacia geral do TJUE, no caso *Schrems II* (processo C-311/18)[29] ao recomendar ao TJUE a sustentação da validade das Cláusulas Contratuais Tipo (SCCs) enquanto mecanismo adequado para a transferência de dados pessoais para fora da UE.

---

[26] Conferido em pesquisa realizada no sítio eletrónicop do Tribunal de Justiça da União Europeia. Disponível em: <https://eurlex.europa.eu/search.html?qid=1593798709005&text=Acordao%20Planet49&scope=EURLEX&type=quick&lang=pt>. Acessado em: 22 de Nov. de 2019.

[27] É um programa de computador usado para adicionar funções a outros programas maiores, provendo alguma funcionalidade especial ou muito específica. Geralmente pequeno e leve, é usado somente sob demanda.Disponível em: <https://www.significados.com.br/url/>. Acessado em: 10 de jan. de 2020.

[28] No âmbito de uma ação inibitória em matéria de direitos dos consumidores, proposta pela Federação alemã das associações de consumidores, foi proferido pelo Tribunal de Justiça o Acórdão Planet491 , que versa sobre (i) o consentimento para instalação de cookies e o valor das opções pré-validadas, (ii) o âmbito de aplicação da obrigatoriedade de recolher o consentimento dos utilizadores previamente à instalação de cookies e a relevância de estarem ou não em causa dados pessoais para que haja esta obrigatoriedade e (iii) sobre a informação que deve ser facultada aos utilizadores aquando da recolha de consentimento, para que se possa considerar que estamos perante informações claras e completas [...]. Disponível em: <https://www.cnpd.pt/home/revistaforum/forum2019_6/96/>. Acessado em: 10 de jan. de 2020.

[29] O caso C-311/18, envolvendo a Data Protection Commissioner, o Facebook e a Maximillian Schrems, foi referenciado à Corte de Justiça da União Europeia pela High Court da Irlanda. Nele foram discutidos a validade das standard contractual clauses como mecanismo para transferência internacional de dados sob a GDPR e a validade do EU-US Privacy Shield (Escudo de Privacidade UE-EUA), normativa criada para regulamentar trocas de dados pessoais entre a União Europeia e os Estados Unidos, para fins comerciais. A decisão proferida pela Corte de Justiça da União Europeia afirmou que as proteções garantidas pelo sistema Privacy Shield não são adequadas, especialmente em razão dos programas de vigilância conduzidos pelos EUA (Surveillance programmes), que nos últimos anos mostrou ser utilizado para além do necessário. Essa decisão tem o condão de alterar a dinâmica de toda a proteção de dados, não apenas dos EUA ou da Europa, mas sim no âmbito internacional. Para acessar este e os demais Acórdãos - Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62018CN0311>. Acessado em: 10 de jan. de 2020.

Feitas estas considerações em relação ao RGPD, e considerando também a relevância dos embates para o aperfeiçoamento e consolidação da lei de proteção de dados brasileira, é de bom alvitre discorrer acerca desta temática igualmente em relação à LGPD, ressalvando-se, contudo, que a análise não se esgota, posto que os estudos em torno da matéria sobre a proteção dos dados pessoais estão presentes no quotidiano das entidades públicas e privadas com vistas ao alcance da conformidade de suas normas.

1.2 Comentários sobre o Seminário de Proteção de Dados Pessoais realizado pela Comissão de Tecnologia, Comunicação e Informática e a Comissão Especial do PL 4060/12, em 22 de Maio de 2018.

A preocupação com a proteção dos dados das pessoas é tema recorrente nos diversos segmentos da sociedade civil no Brasil, aqui entendida em sentido amplo, qual seja, a reunião dos diversos atores que compõem as mais variadas organizações, instituíções, entidades públicas e privadas, as pessoas coletivas e físicas etc.

Como já alhures referenciado no introito deste trabalho, os poderes instituídos constitucionalmente não poderiam ficar alheios ao processo de evolução da TI, o qual contempla em seu bojo a questão delicada do tratamento de dados pessoais e as ferramentas essenciais à sua concretização no campo material. Carece, porém, que a este espaço, o material, esteja associada a criação e aplicação de regras legais que harmonizem de forma adequada e sem intrusão o tratamento dos dados pessoais, sob pena de se infringir direitos fundamentais protegidos pela Constituição Federal do Brasil e algumas leis esparsas, eis que a privacidade está nelas contemplada como objeto de proteção[30].

Tal constatação, provocou o início de incontáveis debates, em princípio no âmbito informal de reuniões, diálogos, matérias de jornais etc, para, num segundo momento, despertar a discussão temática em nível acadêmico e, quase que concomitantemente, o interesse na regulamentação legal por parte dos Poderes Legislativos, ainda que incitados pelos demais Órgãos Estatais de cúpula.

[30] "A Constituição Federal tutela a intimidade e a vida privada, o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas (art. 5º, X e XII) e assegura a concessão de habeas data (art. 5º, LXIX e LXXII). Além disso, o Código de Defesa do Consumidor contém regras específicas sobre bancos de dados e cadastros de consumidores, a Lei 12.414/2011 disciplina o cadastro positivo e a Lei 12.527/2011 regula o acesso a informações públicas. Há, portanto, alguma proteção aos dados pessoais. Mas a limitada aplicabilidade da lei consumerista, nesse aspecto, a jurisprudência restritiva do Supremo Tribunal Federal acerca do habeas data e o sigilo de dados, bem como a ausência de princípios claros a nortear a proteção de dados pessoais indicam que ainda há muito a fazer nos planos doutrinário, legislativo e jurisprudencial para que a proteção de dados pessoais se torne efetiva no Brasil. A edição de lei nacional de proteção de dados é essencial para suprir as omissões hoje existentes e garantir um nível adequado de proteção." In: CUEVA, Ricardo Villas Bôas. *A insuficiente proteção de dados pessoais no Brasil*. Revista de Direito Civil Contemporâneo, São Paulo, 2017. v. 13, ano 4, p. 66.

No Brasil, o tema ganhou maior destaque, especialmente, quando da aprovação do Marco Civil da Internet, instituído pela Lei no 12.965, de 2014[31]. O referido diploma legal deu azo a uma série de reuniões, congressos, seminários, audiências públicas os quais culminaram com propostas de leis e emendas transpondo para o papel preocupações extremamente pertinentes, tais como: a questão da tutela dos dados pessoais e a responsabilidade dos agentes de tratamento; a cristalização de importantes conceitos, como a necessidade de obtenção de consentimento para o tratamento de dados sensíveis e a definição clara dos procedimentos que devem pautar a interconexão de dados entre responsáveis; a não permissão do compartilhamento de dados pessoais com terceiros sem o consentimento "livre, inequívoco, informado, expresso e específico" do titular.

Tais questões foram tratadas no âmbito de uma Comissão Legislativa Especial criada com a finalidade específica de proferir parecer ao Projeto de Lei n° 4060[32], de 2012, o qual dispôs sobre o tratamento de dados pessoais. O retrocitado parecer é de suma importância para o entendimento do processo de aprovação da redação final da LGPD, posto que faz uma abordagem minuciosa dos principais eventos, audiências públicas e seminários que precederam o amadurecimento e o convencimento dos parlamentares acerca da iminente necessidade daquele diploma normativo.

Em seu relatório e precedentemente ao encaminhamento do citado PL, o relator faz uma síntese dos principais pontos abordados no Seminário de Proteção de Dados Pessoais[33] realizado conjuntamente entre a CCTCI e a Comissão Especial do PL n° 4060/12, em 22 de Maio de 2018, e que muito se prestou a subsidiar os diversos substitutivos ao texto original e que restaram constantes na redação da LGPD do Brasil. Assim, é de bom alvitre trazer à baila trechos da síntese textual mencionada, bem como tecer comentários acerca dos principais substitutivos encaminhados à aprovação do texto final da Lei n° 13.709/2018, sobretudo os quem tem pertinência com o presente trabalho.

O supracitado seminário foi aberto pelo então Secretário de Políticas Digitais do MCTIC, Sr. Thiago Lopes, o qual ressaltou "*o desafio e a importância precípua da nova lei – a proteção do usuário e, ao mesmo tempo, não barrar a inovação*". Em relação à aplicação da lei pelo setor público, o Secretário-Executivo do Ministério da Justiça, à época o Sr. Gilson Mendes, destacou que "*o tratamento*

[31] O Marco Civil da Internet, oficialmente chamado de Lei n° 12.965, de 23 de abril de 2014, é a lei que regula o uso da Internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado.Disponível em: <www.planalto.gov.br>. Acessado em: 18 de Dez. 2019.

[32] Parecer ao Projeto de Lei de autoria do Deputado Milton Monti e Relatoria do Deputado Orlando Silva, o qual dispõe sobre o Tratamento de Dados Pessoais. Apensos os PLs n°s 5.276/16 e 6.291/16. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=>. Acessado em: 21 de Dez. de 2019.

[33] O citado Seminário foi organizado em três painéis, cuja síntese pode ser consultada na íntegra do Projeto de Lei n° 4060/2012, que contempla o Projeto de Lei apenso, PL n° 5.276/16, de autoria do Poder Executivo. A síntese está às paginas 26-28, disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=PRL+1+PL406012+%3D%3E> Acessado em: 21 de Dez. de 2019.

de dados pelo setor público deve priorizar as ações de políticas públicas e a integração de seus sistemas", ao tempo em que, o então Presidente da CCTCI, Deputado Goulart, destacou *"a importância do debate para o futuro de oportunidades que se descortina"*[34].

Cabe destacar os temas abordados no painel sobre "Abordagem regulatória para o tratamento de dados pessoais", no qual o Secretário do MCTIC mencionou "*a importância da Estratégia Brasileira de Economia Digital, e que a criação de um ente deveria ser cotejada com o limite de gastos e que o excesso regulatório pode representar exportação de oportunidades*". O Secretário de Tecnologia da Informação e Comunicação do MPOG destacou "*a inciativa da ferramenta gov-data, útil para o cruzamento e checagem do grande volume de informações guardadas pelos órgãos públicos*", ao passo que o Sr. Frederico Ceroy, Promotor de Justiça e Coordenador da Comissão de Proteção de Dados do MPDFT, ressaltou que "*uma regulamentação detalhada é positiva e que a autoridade deveria ser concentrada em uma única pessoa, rodeada de engenheiros e poliglotas*".

O Diretor-Presidente do NIC.br[35], Demi Getschko, "*destacou a característica multissetorial da atividade e que a regulação deve prever a dinâmica colaborativa, como também ponderou que a aplicação dos dados deve ser transparente e ética, uma vez que a tendência é de que os dados vazem, em algum momento*". O representante da Direção Geral da Justiça e Consumidores da União Europeia, à época o Sr. Bruno Gencarelli, "*destacou que a regulamentação deve ser adaptativa à tecnologia e que o Brasil é um importante ator no fluxo internacional de dados"*. Ao final deste painel, foi salientado a pesquisa com dados sensíveis e a agregação de dados oriundos de amostras massivas gera oportunidade de construção de políticas públicas.

"*O uso de dados pessoais como instrumento de campanha eleitoral e a persuasão da opinião pública"* foi tratado no segundo painel, ocasião em que foi abordada a importância da segmentação de personalidades para fins de propaganda eleitoral, como também a representante do *Facebook*, Sra. Nathalie Gazzaneo, oportunamente esclareceu que "*a plataforma não vende dados pessoais, que o foco do trabalho da empresa está na sua transparência e que no episódio da Cambridgy Analytica*[36] *443 mil*

---

[34] Idem.

[35] O Núcleo de Informação e Coordenação do Ponto BR é uma associação, sem fins lucrativos, criada 08 de março de 2005 para implementar as decisões e os projetos do Comitê Gestor da Internet no Brasil – CGI-br, que é o responsável por coordenar e integrar as iniciativas e serviços da internet no Brasil. Disponível em: <https://www.nic.br/> .Acessado em: 14 de Dez. de 2019.

[36] Cambridge Analytica Ltda. foi uma empresa privada que combinava mineração e análise de dados com comunicação estratégica para o processo eleitoral. Foi criada em 2013, como um desdobramento de sua controladora britânica, a SCL Group para participar da política estadunidense. A Cambridge Analytica trabalhou para a campanha eleitoral do presidente americano, Donald Trump, se declarou culpada por ter se negado a revelar dados pessoais que tinha extraído do Facebook. A empresa foi condenada por um tribunal de Londres a pagar multa de 15 mil libras (US$ 19,1 mil ou 16,7 mil euros) e os custos do processo, no valor de 6 mil libras. O Facebook já havia admitido que a Cambridge utilizara um aplicativo para coletar informações privadas de 87 milhões de usuários sem seu conhecimento. A empresa

brasileiros foram atingidos e que 200 aplicativos estariam sendo revisados". Bruna Santos, representante da Coalização Direitos na Rede[37], "*defendeu a transparência na publicidade e o combate ao discurso de ódio"*. O Doutor Paulo M. R. Brnacher, Professor titular da Pontifícia Universidade Católica de São Paulo - PUC/SP, "*destacou a dificuldade das plataformas serem neutras e que a educação do eleitor deve ser reforçada para que este melhor reflita sobre táticas de convencimento"*. Importante ponto foi a assertiva de Gustavo Artese, Mestre em Direito pela Universidade de Chicago e Chair KnowledgeNET da Associação Internacional de Profissionais de Privacidade - IAPP, ao destacar "*a fadiga do consentimento e que a lei deve ser principiológica"*.

O Seminário foi finalizado trazendo à tona um tema bastante atual e preocupante, qual seja, o "tratamento a notícias falsas - *fake news*". Neste painel deu-se destaque aos "*fact-checkers*"[38] que, segundo Natalia Viana, Codiretora da Agência Pública, *"são uma tendência em crescimento e que há um processo de certificação internacional.* Na ocasião, o representante do *Google* no evento, Marcelo Lacerda, ponderou o uso generalizado deste termo, que "*prefere o uso do termo desinformação*", e "*ressaltou a importância do jornalismo e da educação dos usuários"*. No tocante ao tema, o Professor Fábio Gouveia, do Laboratório de Estudos sobre Imagem e Cibercultura – Labic, da Universidade Federal do Espírito Santo - UFES, "*explicou o apelo desse tipo de notícias e asseverou que o jornalismo precisa se adaptar a enfrentar as bolhas ideológicas*"[39].

Por fim, cabe ressaltar importantes contribuições levadas em conta na proposição do PL n°

---

depois utilizou estes dados para mandar aos usuários publicidade política especialmente adaptada e elaborar informes detalhados para ajudar Trump a ganhar a eleição contra a candidata democrata Hillary Clinton. Disponível em: <https://www.jusbrasil.com.br/topicos/187366730/cambridge-analytica >. Acessado em: 14 de Dez. de 2019.

[37] A Coalizão Direitos na Rede é uma rede independente de organizações da sociedade civil, ativistas e acadêmicos em defesa da Internet livre e aberta no Brasil. Formada em julho de 2016, busca contribuir para a conscientização sobre o direito ao acesso à Internet, a privacidade e a liberdade de expressão de maneira ampla. O coletivo atua em diferentes frentes por meio de suas organizações, de modo horizontal e colaborativo. Disponível em: <www.direitosnarede.org.br>. Acessado em:17 de Dez. de 2019.

[38] O *fact-checking* é uma checagem de fatos, isto é, um confrontamento de histórias com dados, pesquisas e registros. Se um político jura que nunca foi acusado de corrupção, há registros judiciais que irão atestar se é verdade. Se o governo diz que a inflação diminuiu, é preciso checar nos índices se isso realmente ocorreu. E se uma corrente diz que há um projeto de lei para cancelar as eleições, é preciso conferir nas propostas em tramitação se essa informação é real. O *fact-checking* é uma forma de qualificar o debate público por meio da apuração jornalística. De checar qual é o grau de verdade das informações. Reportagens do Buzzfeed e do The Guardian, por exemplo, mostraram que boa parte do conteúdo compartilhado na internet durante as últimas eleições nos Estados Unidos vieram de sites de notícias falsas. Situação semelhante aconteceu no Brasil na semana do impeachment de Dilma Rousseff. Disponível em: <https://pt.wikipedia.org/wiki/Verifica%C3%A7%C3%A3o_de_fatos>. Acessado em: 15 de Out. de 2019.

[39] A personalização pela ação de algoritmos de informações, filmes e músicas oferecidos nas grandes plataformas como *Google, Facebook, WhatsApp, Twitter, Instagram* e outras como *Netflix e Spotfy*, leva as pessoas a serem expostas, cada vez mais, a opiniões e ideias similares às suas próprias visões de mundo. O efeito dessas bolhas ideológicas, conhecido como "bolha online" *(filter bubble)* ou "câmara de ecos", sobre as sociedades democráticas ainda não é conhecido por completo. Fonte: <https://jornalggn.com.br/eleicoes/bolhas-ideologicas-ou-camaras-de-eco-por-fernando-nogueira-da-costa>. Acessado em: 17 de ez. de 2019.

4060/2012, tais como a responsabilização dos grandes grupos da internet, bem como a necessidade de fortalecimento da educação, além da ênfase dada à questão da desinformação como fator que prejudica a democracia.

Como mencionado nas linhas precedentes, foram de suma importância as diversas reuniões, contribuições, debates etc motivados pelo tema "proteção de dados pessoais", que se arrastaram pelo Brasil a partir de novembro de 2010. Neste sentido, foi de grande relevância o Projeto de Lei n° 4.060/2012, de autoria do Deputado Federal Milton Monti, e do Projeto de Lei n° 5.276/16 àquele apensado, de iniciativa do Poder Executivo Federal, da então Presidente Dilma Rousseff. Em 2018, o Plenário do Senado aprovou o Projeto de Lei n° 53/2018 (na Câmara dos Deputados sob o n° 4060/2012)[40] enviado pela Câmara, o qual culminou com a sanção da Lei Geral de Proteção de Dados, Lei n° 13.709, de 14 de agosto de 2018.

O referido projeto foi produto do trabalho desenvolvido durante cinco anos no Ministério da Justiça, por meio da Secretaria Nacional do Consumidor - SENACON e, para a sua elaboração, foram realizadas diversas reuniões técnicas e setoriais, além de dois debates públicos pela *Internet*, em 2010 e 2015, que resultou em mais de 2.000 contribuições dos diversos setores envolvidos. Tais propostas se inserem em um contexto mundial, que se sobrepõem às legislações nacionais de cada país, de forma a tratar da questão dos dados pessoais e garantir a proteção das pessoas de maneira harmônica. Com efeito, a construção de um arcabouço similar entre os países gera um ambiente propício aos negócios, principalmente globais, oriundos do manuseio de dados, e se põe em sintonia com a Resolução da ONU, de 25 de novembro de 2013, sobre "Direito à Privacidade na Era Digital". Naquele contexto, conforme consta da mensagem do Poder Executivo Federal, "*109 países já possuiam normas nesse sentido e mais de 90 destes tinham uma autoridade pública específica especializada no tema*"[41].

Tendo em conta o explicitado no presente item e considerando que dados e informações se tornaram insumos de negócios e movimentam poderosíssimas indústrias globais, associada à necessidade de inserir o Brasil em um ambiente integrado com o mundo e, portanto, propício para o desenvolvimento do setor, ao encaminhar o PL n° 5276/2016 apensado ao PL n° 4060/2012, com o respectivo parecer de aprovação, a Comissão Especial concluiu por introduzir diversos melhoramentos ao texto, submetendo um substitutivo às proposições, os quais, posteriormente, sofreram alterações com a publicação da Medida Provisória n° 869, de 27 de dezembro de 2018, e da Lei n° 13.853, de 8 de julho

[40] Ver tramitação da matéria com dados disponíveis em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/133486>. Acessado em: 17 de dez. de 2019.

[41] O texto compõe o voto do Relator do Projeto de Lei n° 4060/2012, Deputado Orlando Silva. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=PRL+1+PL406012+%3D%3E+PL+4060/2012>, p.6-7. Acessado em: 17 de dez. de 2019.

de 2019, sobre os quais dedicar-se-ão as linhas que se seguem, de forma a melhor compreensão da LGPD do Brasil.

A ementa a Lei n° 13.853/2019 trouxe a denominação "Lei Geral de Proteção de Dados Pessoais" e incluiu o parágrafo único[42] ao Art. 1°, com o objetivo de ampliar o seu alcance para os Estados, o Distrito Federal e os Municípios, além de incluir o inciso III ao Art. 3°, considerando objeto de tratamento os dados pessoais que forem coletados no território nacional, independentemente do meio; a seu turno, o substitutivo incluiu entre os fundamentos da disciplina de proteção de dados o inciso VII ao art. 2°, segundo o qual os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania são diretamente afetados pelo tratamento de dados pessoais realizados pelos diversos setores, com consequências em variados aspectos da vida em sociedade[43].

No tocante ao tratamento de dados pessoais realizado para fins exclusivo de segurança pública e defesa nacional, ante a relevância da matéria, e em consonância com as legislações de outros países, o §1° do Art. 4° atribui à Lei específica a previsão do atendimento do interesse público para esse tipo de tratamento. Entendeu-se, ainda, que devido à natureza crítica para a soberania e segurança das pessoas e das instituições, em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público, conforme redação do § 4° do mesmo artigo[44].

Com relação às definições da Lei, notadamente o que consta do art. 5°, o entedimento a que se chegou pode ser assim resumido: a) os dados sensíveis (inciso II) devem exigir a obtenção do consentimento específico e em destaque por parte do titular dos dados, porém aplica-se apenas aqueles relacionados a pessoas naturais. Desta forma, dados genéticos oriundos de plantas - de interesse do agronegócio ou da chamada agricultura de precisão, por exemplo - ou anonimizados excluem-se do conceito; b) às definições constantes dos incisos III e XI passaram a ter uma relativização temporal e tecnológica; assim, os dados serão considerados anonimizados quando utilizadas técnicas razoáveis e disponíveis à época de seu tratamento. O entedimento provém do fato de que a anonimização é passível de ser revertida em determinadas situações, posto que a anonimização de dados de hoje poderá se tornar obsoleta amanhã; c) o "relatório de impacto à proteção de dados pessoais" (inciso XVII) deverá conter a

[42] Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. (Incluído pela Lei nº 13.853, de 2019). Disponível em: <https://www.camara.leg.br/proposicoesWeb/>. Acessado em: 17 de dez. de 2019.

[43] O texto compõe o voto do Relator do Projeto de Lei n° 4060/2012, Deputado Orlando Silva. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=PRL+1+PL406012+%3D%3E+PL+4060/2012>. p.31. Acessado em: 20 de dez. de 2019

[44] Ibid. P. 31.

documentação dos processos que possam gerar risco, além de medidas de mitigação; d) os "órgãos de pesquisa" (XVIII) de ciência, tecnologia e inovação, de natureza pública ou privada sem fins lucrativos devem ter como missão institucional a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e) a autoridade nacional (XIX) é instituição que deverá integrar a administração pública e terá a atribuição de zelar, implementar e fiscalizar o cumprimento da Lei em todo território nacional[45].

No que se refere às hipóteses de tratamento de dados pessoais[46], o art. 7° e o Art. 8° fixam importantes regras a serem observadas, principiando pela obtenção de consentimento escrito e por livre manifestação do titular, o qual poderá ser ainda específico no caso de obtenção pelo controlador, conforme § 5° do Art. 7°. A previsão do tratamento de dados quando do cumprimento de obrigação legal, regulatória, contratual, estudos, processos judiciais, administrativo ou arbitral, bem como para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária. Em atenção ao art. 43 do CDC, o inciso X passa a prever a recepção expressa da possibilidade de abertura de cadastro de consumidores para proteção do crédito. Para os casos em que o próprio titular torna parte de seus dados manifestamente públicos, o § 4° prevê a dispensa da obtenção do consentimento, resguardados os direitos do titular e demais princípios da Lei, a exemplo da solicitação de exclusão de dados ou suspensão do tratamento. O § 5° estabelece que na transferência de dados para outros responsáveis, como no caso de empresas do mesmo e de outros grupos empresariais que realizam o compartilhamento de dados coletados de titulares, os quais torna possível a perda do controle do titular sobre seus próprios dados, será necessária a obtenção de consentimento específico para esse fim.

Com o objetivo de garantir a eficácia das garantias dadas ao usuário, o inciso V do art. 9° estabelece que somente será necessário comunicar ao titular os casos em que os dados forem efetivamente compartilhados com terceiros responsáveis, quando devidamente consentido, evitando-se, desta forma, a necessidade de consentimentos constantes. Além disso, o § 2° dá a garantia de proteção no sentido de que o titular seja informado a cada vez que surgirem novas finalidades para o tratamento dos dados, não compatíveis com o consentimento original[47].

---

[45] Ibid, p. 31-32.

[46] O texto compõe o voto do Relator do Projeto de Lei n° 4060/2012, Deputado Orlando Silva. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=PRL+1+PL406012+%3D%3E+PL+4060/2012>. p.33-34. Acessado em: 20 de dez. de 2019.

[47] O texto compõe o voto do Relator do Projeto de Lei n° 4060/2012, Deputado Orlando Silva. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=PRL+1+PL406012+%3D%3E+PL+4060/2012>, p.33-34. Acessado em: 20 de dez. de 2019.

Inspirado nas práticas europeias que remonta a 1995, o art. 10 trata do legítimo interesse, qual seja, a hipótese de tratamento de dados pessoais sem a necessidade de prévia obtenção do consentimento. Tal regra, além de evitar que o titular dos dados seja onerado ao extremo, é importante igualmente por atender a uma finalidade pública ou a uma finalidade privada legítima, a exemplo da prevenção a fraudes bancárias ou a garantia de segurança das redes. Contudo, o legítimo interesse deverá se basear em situação concreta e desde que atendidas as legítimas expectativas do titular, além de sempre serem observados os princípios da adequação, necessidade e transparência bem como da possibilidade de fiscalização[48].

Para efeitos de tratamento, devido a existência de duas categorias de dados e tendo em vista que os dados sensíveis inserem-se entre os dados pessoais, o substitutivo discriminou os tipos de consentimento. Assim, para os dados pessoais gerais, o consentimento é livre, informado e inequívoco. Contudo, o art. 11 prevê que esse consentimento deverá ser específico e em destaque para finalidades específicas, ou seja, adicionais às contidas no consentimento referente ao tratamento de dados pessoais "gerais". Destarte, a necessidade de se obter consentimento diferenciado torna-se um adicional de proteção para este tipo de dados, razão pela qual foi incluída as alíneas f) e g), ao inciso II[49], que contêm as exceções à necessidade de obtenção de consentimento específico, excetuando da obrigação de obtenção de consentimento também para estes casos[50].

O § 4° do mesmo Art. 11, com a redação dada pela Lei n° 13.853/2019 incluiu importante vedação à comunicação ou ao uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde, quando o objetivo for obter vanfagens econômicas, ecetuando-se os casos de prestação de serviços de saúde de assistência farmacêutica e de assistência à saúde, e para pemissão da portabilidade de dados solicitada pelo seu titular e das transações financeiras e administrativas resultantes do uso e da prestação destes serviços.

---

[48] Ibid, p. 34.

[49] Seção II

Do Tratamento de Dados Pessoais Sensíveis

Art.11.O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

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. Disponível em: <www.senado.gov.br> . Acessado em: 23 de dez. de 2019.

[50] O texto compõe o voto do Relator do Projeto de Lei n° 4060/2012, Deputado Orlando Silva. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=PRL+1+PL406012+%3D%3E+PL+4060/2012>, p.35. Acessado em: 23 de dez. de 2019.

No que diz respeito aos dados anonimizados, ainda que o conceito tenha sido relativizado, conforme visto no artigo dedicado às definições, o § 1° do Art. 12 prevê que sejam considerados fatores objetivos, tais como tempo, custo, tecnologias disponíveis no momento e a utilização exclusiva de meios próprios, ao passo que a leitura do § 2° nos remete a considerar dados pessoais aqueles utilizados para a formação do perfil comportamental de uma determinada pessoa natural apenas se a pessoa for identificada.

Aos dados relativos à saúde reporta-se o Art. 13, que acertadamente permite aos órgãos de pesquisa o acesso a estes dados para a realização de estudos em saúde pública, desde que para uso exclusivo dentro dos órgãos, para a finalidade específica de pesquisa e quando mantidos em ambiente controlado e seguro. Tais dados deverão ser, sempre que possível, pseudononimizados ou anonimizados e veda-se a revelação do resultado dos dados pessoais obtidos. Ademais, ante a notável complexidade dos procedimentos, protocolos e códigos de conduta, a dispersão dos bancos de dados e a variedade de atores envolvidos com este tipo de tratamento, seja em nível público ou privado, há a permissão para que o órgão regulador, bem como as autoridades de saúde possam emitir regramentos específicos, no âmbito de suas competências. Neste sentido, o inciso III do Art. 15 impede a exclusão de dados que sejam de interesse público[51].

Segundo o § 7° do Art. 18, ao titular dos dados foi retirado o direito à portabilidade de dados anonimizados já tratados pelo controlador, porém foram acrescentados direitos antes não previstos, a saber: o direito de peticionar junto ao responsável expresso pelo § 1°; a 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 industria o de informação das entidades públicas e privadas com as quais o responsável realizou uso compartilhado de dados (inciso VII) e de informações sobre a possibilidade de não fornecer o consentimento e sobre as consequências de eventual negativa de consentimento (VIII); o direito à revogação do consentimento nos termos do §5° do art. 8° (IX)[52]; e o direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões que definem o perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade do titular dos dados,

[51] O texto compõe o voto do Relator do Projeto de Lei n° 4060/2012, Deputado Orlando Silva. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=PRL+1+PL406012+%3D%3E+PL+4060/2012>, p.35. Acessado em: 20 de dez. de 2019.

[52] Art. 8º ...

§ 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. Disponível em: www.senado.gov.br . Acessado em: 23 de dez. de 2019

conforme Art. 20.

Outro ponto importante a ser ressaltado, diz respeito à transferência internacional de dados, notadamente o disposto nos Arts. 33 a 36, do Capítulo V da LGPD. Pela leitura do inciso I do Art. 33, consideram-se como sujeito da transferência internacional de dados os países estrangeiros e as organizações internacionais, as pessoas jurídicas de direito internacional público, que proporcionem grau de proteção de dados pessoais adequado ao previsto na LGPD, facilitando a transferência de dados, essencial às atribuições dessas entidades multilaterais. Verifica-se também que o uso do termo "proteção adequada" ao invés de "proteção equiparável", foi mais apropriado, eis que se afasta a ideia de comparação do grau de proteção mais restrita e menos ambígua[53].

No inciso II do art. 33 inseriu-se outras formas de reconhecimento de proteção de dados pessoais pelo órgão competente, a saber: cláusulas contratuais específicas para uma determinada transferência, cláusulas contratuais padrão, normas corporativas globais, e a emissão de selos, certificados ou códigos de conduta e adequação, emitidos por organismos internacionais, a exemplo do que vem sendo adotado por outros países.

Devido a relevância desse tipo de transferência, duas formas de tratamento foram dadas ao consentimento: a do inciso VIII do Art. 33, pelo qual o consentimento deve ser específico e em destaque; ao passo que o inciso IX permite a transferência internacional, ainda que sem consentimento, nas hipóteses de cumprimento de obrigação legal ou regulatória pelo responsável, para a execução de um contrato ou de procedimentos preliminares de um contrato do qual é parte o titular, e para o exercício regular de direitos em processo judicial, administrativo ou arbitral. Além disso, com a inserção do parágrafo único ao Art. 33, passou a existir a previsão da possibilidade de pessoas jurídicas de direito público e responsáveis, em determinadas condições, requererem ao órgão competente a avaliação do nível de proteção a dados pessoais conferido por país ou organização internacional. Conforme consta do Art. 34, em todas as situações, deve ser observada a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais[54].

---

[53] O texto compõe o voto do Relator do Projeto de Lei n° 4060/2012, Deputado Orlando Silva. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=PRL+1+PL406012+%3D%3E+PL+4060/2012>. p.39. Acessado em: 20 de dez. de 2019.

[54] Nos seguintes termos, consta do voto: "*No inciso VIII do art. 33 aditamos a obrigação de o consentimento ser específico e em destaque para a transferência internacional, em razão da importância que envolve esse tipo de transferência. Em seguida, acrescentamos inciso IX ao art. 33 para permitir a transferência internacional, ainda que sem consentimento, nas hipóteses de cumprimento de obrigação legal ou regulatória pelo responsável, para a execução de um contrato ou de procedimentos preliminares de um contrato do qual é parte o titular, e para o exercício regular de direitos em processo judicial, administrativo ou arbitral. Inserimos parágrafo único ao art. 33 para prever a possibilidade de pessoas jurídicas de direito público e responsáveis, sob determinadas condições, requererem ao órgão competente a avaliação do nível de proteção a dados pessoais conferido por país ou organização internacional*". Disponível em:

Fechando este conjunto normativo relativo à transferência de dados internacionais, duas importantes regras foram estabelecidas: a do Art. 35, o qual habilita a autoridade nacional a definir o conteúdo de cláusulas contratuais padrão e a proceder à verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais, selos, certificados e códigos de conduta, bem como requerer informações suplementares ou realizar diligências de verificação quanto às operações de tratamento, além de poder designar organismos de certificação, que estarão sob sua fiscalização; a do Art. 36, o qual assegura a manutenção dos direitos dos titulares no âmbito da transferência internacional de dados, ao dispor que quaisquer alterações nas garantias apresentadas pelo responsável deverão ser comunicadas à autoridade nacional[55].

As figuras dos agentes de tratamento de dados pessoais, quais sejam, o Controlador, o Operador e o Encarregado, bem como suas atribuições e responsabilização e ressarcimento pelos danos patrimonial, moral, individual ou coletivo, que vierem a ser causados a outrem, em razão do exercício de atividade de tratamento de dados pessoais são tratadas no Capítulo VI da LGPD[56].

No tocante às sanções administrativas a serem aplicadas por descumprimento dos preceitos legais da LGPD (Arts. 52 a 54), em relação às entidades e órgãos públicos, verifica-se ser possível a aplicação das sanções de advertência, publicização da infração, bloqueio e eliminação de dados pessoais, suspensão parcial ou total de funcionamento de banco de dados, suspensão do exercício de atividade de tratamento e a proibição parcial ou total do exercício dessas atividades.

A criação de um órgão técnico competente, centralizado e com independência e autonomia administrativa e financeira para expedir normas complementares e fiscalizar o setor foi objeto de muitos debates, bem como de longo trâmite legislativo, em meio a emendas, vetos, enfim, a forma de enquadramento na estrutura administrativa federal e de escolha dos seus dirigentes, bem como a gestão

---

<https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=PRL+1+PL406012+%3D%3E+PL+4060/2012>, p.39. Acessado em: 23 de dez. de 2019.

[55] O texto compõe o voto do Relator do Projeto de Lei n° 4060/2012, Deputado Orlando Silva. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=PRL+1+PL406012+%3D%3E+PL+4060/2012>, p.39. Acessado em: 23 de dez. de 2019.

[56] Neste sentido, Oliveira e Cots afirmam que "*a responsabilidade civil dos agentes de tratamento segue a regra geral estabelecida pelos artigos 186, 187 e 927 do Código Civil Brasileiro:*

Art. 186. Aquele que por ação ou omissão voluntária, negligência ou imprudência, violar direitoe causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.

Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.

Art.927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo".

E seguem: "o nexo causal do dano está intrinsecamente ligado à violação da LGPD, sendo que, se não houve violação, não se torna aplicável o artigo 42, não se configurando ato ilícito". COTS, Márcio; OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Pessoais comentada. 2.ed.rev.atual. e ampl.- São Paulo: Thomson Reuters . Brasil, 2019. p. 175

de seus recursos humanos, aos ditames estabelecidos pela Lei das Agências Reguladoras, Lei n° 9.986, de 18 de julho de 2000.

Não é intenção deste trabalho apresentar um histórico que retrate as etapas vencidas até se chegar a escolha da atual denominação do órgão técnico competente com as atribuições especificadas no Art. 55-J da LGPD, qual seja, a ANPD (Art. 55-A). Convém, contudo, registrar a informação de que somente com a edição da Lei n° 13.853, de 8 de julho de 2019, sancionada pelo Presidente Jair Messias Bolsonaro, com vetos parciais, pacificou-se o entendimento acerca da importância da criação de um Órgão competente com atribuíções objetivamente definidas em lei e dotado de ferramentas regulatórias adequadas ao alcance do exercício fiscalizatório.

A retrocitada Lei n° 13.853/2019, que alterou a ementa da Lei nº 13.709[57], de 14 de agosto de 2018, fazendo nela constar a denominação Lei Geral de Proteção de Dados Pessoais[58], resultou do Projeto de Lei de Conversão nº 7/2019 da MP nº 869/2018, aprovada pelo Senado Federal, e trouxe em seu bojo alterações significativas[59], entre as quais se destacam:

I – A previsão de que a proteção de dados é de interesse nacional, evitando a proliferação de leis estaduais e municipais que venham tentar regular a matéria;

II – A criação da ANPD, em princípio Órgão integrante da Presidência da República, podendo ter, após dois anos, a sua natureza jurídica alterada e até, eventualmente, transformada em entidade da administração pública federal indireta, submetida a regime autárquico especial;

III – O encarregado de dados, também conhecido como *Data Protection Officer (DPO),* poderá ser uma pessoa jurídica, e sua indicação caberá ao controlador e também ao operador;

IV – Direito do titular dos dados pessoais a obter do controlador a 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;

V – Incremento na lista de penalidades, havendo a possibilidade de: (i) suspensão

---

[57] Lei que alterou o Marco Civil da Internet (Lei nº 12.695/2014) e foi originada do PL nº 4060/2012 – CD, o qual recebeu no Senado Federal o nº 53/2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>, Acessado em 11 de Nov. de 2019.

[58] Art. 1º. A ementa da Lei nº 13.709, de 14 de agosto de 2018, passa a vigorar com a seguinte redação: "Lei Geral de Proteção de Dados Pessoais (LGPD)". Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>, Acessado em: 11 de Nov de 2019.

[59] Alteraçoes especificadas no artigo: "As últimas mudanças na Lei Geral de Proteção de Dados". Disponível em: <https://www.lgpdbrasil.com.br/confira-as-ultimas-mudancas-na-lei-geral-de-protecao-de-dados/>. Acessado em: 14 de dez. de 2019.

parcial do funcionamento do banco de dados pelo período de 6 (seis) meses, prorrogável por igual período, até a regularização por parte do controlador; (ii) suspensão do tratamento dos dados pessoais pelo período de 6 (seis) meses, prorrogável por igual período; e (iii) proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados por entidades infratoras, incluindo poder público. Essas três sanções apenas poderão ser aplicadas após já ter sido imposta ao menos uma das seguintes sanções: multa simples, multa diária, publicização da infração; bloqueio dos dados pessoais e eliminação dos dados pessoais;

VI – Possibilidade da desobrigação do controlador informar aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados sobre a necessidade de correção, eliminação, anonimização ou o bloqueio dos dados, no caso de ser comprovadamente impossível ou que implique esforço desproporcional;

VII – Possibilidade do tratamento da totalidade dos dados pessoais de bancos de dados de fins exclusivos da segurança pública, defesa nacional, segurança do Estado ou de atividades de investigação e repressão de infrações penais, por pessoa de direito privado cujo capital é integralmente constituído pelo poder público;

VIII – Possibilidade de utilização dos dados de acesso público ou tornados públicos pelo titular, pelos controladores para finalidades distintas daquelas para as quais o dado foi publicado, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios da lei;

IX – Possibilidade da transferência de dados pessoais de responsabilidade do poder público para entidades privadas, nas seguintes hipóteses: a) houver previsão legal ou em instrumentos jurídicos administrativos; b) a transferência for para fins de prevenção à fraude, segurança e integridade do titular dos dados; e c) os dados forem publicamente acessíveis;

X – Previsão da possibilidade de compartilhamento dos dados de saúde para fins de obtenção de vantagem econômica, desde que a finalidade seja a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, aí incluídos os serviços auxiliares de diagnose e terapia, e sob a condição de que seja em benefício dos interesses dos titulares de dados. Além disso, fica permitida também a inclusão dos serviços de saúde na tutela da lei;

XI – Visando resguardar os dados dos usuários, a lei passou a vedar expressamente a utilização de dados para fins de análise de riscos e para fins de contratação ou para exclusão de beneficiários pelos planos de saúde e empresas de assistência à saúde;

XII – Direito assegurado ao titular dos dados de 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.

Com as alterações implementadas pela Lei n° 13.853, de 8 de julho de 2019, a nova LGPD apresenta em seu texto o capítulo IX, que incluiu a Autoridade Nacional de Proteção de Dados[60] e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD), o qual está subdividido em duas seções que tratam da ANPD (Arts. 55-A ao 55-L) e do CNPD (Arts. 58-A e 58-B), respectivamente.

Por fim, e considerando o escopo deste trabalho, o qual busca contextualizar a adequação do TC. de Portugal, do TCE/PB e do TCE/RN às regras das respectivas legislações sobre a proteção de dados pessoais no âmbito de suas atuações, enquanto Entidades de fiscalização da escorreita aplicação dos recursos públicos, há de se fazer uma distinção no tocante ao momento de aplicação do RGPD e da LGPD.

Com efeito, o RGPD da União Européia encontra-se em plena vigência e as Entidades Públicas, a exemplo do Tribunal de Contas de Portugal, estão "a todo vapor" promovendo os ajustes e adequações de suas normas internas necessários ao seu cumprimento. De outra banda, no Brasil, com a publicação da Lei n° 13.853, de 8 de julho de 2019, que alterou a Lei n° 13709, de 14 de agosto de 2018, dois períodos de vacância foram estabelecidos, conforme o Art. 65[61].

Verifica-se que o inciso I do Art. 65 põe em relevância os artigos relativos à Autoridade Nacional de Proteção de Dados, ao estabelecer a vigência na data de 28 de

---

[60] A Autoridade Nacional de Proteção de Dados Pessoais tem sido alvo de polêmicas desde a sua formulação no Congresso. Dois argumentos colidiram em 2018. De um lado, o argumento da escassez: diante da situação econômica do país e da ausência de recursos suficientes para criação de mais uma agência reguladora, seria preciso pensar em alternativas, distribuindo as funções da Autoridade entre órgãos já existentes. Do outro, o argumento da capacidade regulatória: a autonomia e independência da Autoridade são o comum na experiência internacional, vez que asseguram maior confiança e qualidade técnica em Autoridades independentes e autônomas. Nessa disputa, a solução encontrada foi um caminho intermediário. Por um período potencialmente provisório, a ANPD estará ligada à estrutura da Presidência, com vinculação à administração pública direta. Com isso, parte de seu *staff* poderá ser constituído de cargos já previstos na estrutura do governo. Aposta-se, no entanto, em uma suposta independência de facto: fica assegurada autonomia decisória e há promessa de que não haverá interferência no trabalho do Conselho Diretor, formado por profissionais com capacidade técnica demonstrada e empossados após sabatina no Senado. Disponível em: <https://cnbpr.org.br/2019/07/11/artigo-as-mudancas-finais-da-lei-geral-de-protecao-de-dados-pessoais/>. Acessado em: 14 de dez. de 2019.

[61] Art. 65. Esta Lei entra vigor:

I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e

II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. Disponível em: <www.planalto.gov.br>. Acessado em: 20 de dez. de 2019.

dezembro de 2018 e, para os demais artigos um vacatio legis de 24 meses contados da data da publicação.

A explicação para esta diferenciação nos remete à Medida Provisória nº 869/2018, de iniciativa do ex-Presidente Michel Temer, cujo texto resultou no Projeto de Lei de Conversão nº 7/2019 e consequente Lei nº 13.853/2019. O novo prazo para entrada em vigor da LGPD foi estendido pela citada medida provisória, desconsiderando a regra de contagem contida no § 3º, do artigo 1º, da Lei de Introdução às normas do Direito Brasileiro (LINDB)[62], o que se levou a pensar que a lei entraria em vigor em 16 de agosto de 2020.

Contudo, conforme preceitua o citado § 3º, contados os vinte e quatro meses, a partir de 28 de dezembro de 2018 (data de publicação da MP nº 869/2018, que deu nova redação ao artigo 65 da LGDP), conclui-se que a LGPD entrará em vigor em 29 de dezembro de 2020 e não em 16 de agosto, tal como ocorreria se o prazo pudesse ser contado a partir da data original da publicação da lei.

O objetivo da *vacatio legis* é propiciar tempo suficiente para o conhecimento da lei, logo, aplica-se o § 3º do artigo 1º da LINDB quando as alterações não sejam meras correções. No dizer jurídico: "*Ubi eaden ratio, ibi eaden legis dispositio* (onde a razão é a mesma, a lei deve ser a mesma)". Eis o por que do escalonamento da vigência de dois conjuntos de dispositivos segundo duas regras distintas, revogando-se a redação do texto original da LGPD, o qual estabelecia *vacatio legis* único de 18 meses.

Ante o impacto da aplicação da nova LGPD, pode-se dizer que a alteração no período de início da vigência vem tão somente beneficiar os destinatários, notadamente sob a perspectiva dos Órgãos e Entidades da Administração Pública, os quais passam a dispor de um período mais elástico para adequar as suas normas internas às disposições da Lei nº 13.709/2018, com as alterações introduzidas pela Lei nº 13.853/2019, bem como a canalização de recursos orçamentários para o atendimento das exigências legais no que se refere à aquisição de equipamentos e toda a logística tecnológica aí envolvida.

[62] Art. 1°. Salvo disposição contrária, a lei começa a vigorar em todo o país quarenta e cinco dias depois de oficialmente publicada.

§ 2° ...

§ 3° Se, antes de entrar a lei em vigor, ocorrer nova publicação de seu texto, destinada a correção, o prazo deste artigo e dos parágrafos anteriores começará a correr da nova publicação.

§ 4° As correções a texto de lei já em vigor consideram-se lei nova. Disponível em: <www.planalto.gov.br>. Acessado em: 20 de dez. de 2019.

1.3 Conceitos Gerais aplicáveis à proteção de Dados Pessoais

A inclusão do Poder Público, representado pelas Entidades que executam as políticas públicas e pelos Órgãos que lhes asseguram o cumprimento, no escopo do Regulamento Geral sobre Proteção de Dados - RGPD e da LGPD, obriga-o a adequar-se a estes diplomas normativos e requer o conhecimento de novas tecnologias, a mudança de paradigma e o investimento em segurança e proteção de dados, outrora negligenciados ou esquecidos.

Desta forma, com as regras implementadas pelas sobreditas legislações de proteção de dados pessoais, as autoridades públicas viram-se no dever não apenas de atuar de forma a evitar a comercialização de dados pessoais para fins diferentes daqueles aos quais foram coletados, mas, sobretudo, tiveram de incorporar ao ambiente de trabalho e à mentalidade de seus colaboradores (servidores públicos, funcionários, contratados etc) novos conceitos relacionados à proteção de dados, sobre os quais dedicar-se-á algumas linhas, notadamente aqueles mais debatidos na doutrina e em virtude dos quais se debruçam os TC's ao estudo e integração as suas normas internas.

As Entidades Públicas, aí incluídos os TC's, não poderiam ficar indiferentes ante o crescente avanço das novas tecnologias e de novos conceitos, tendo em conta principalmente o advento da internet e da cibercultura, que tem provocado mudanças significativas na sociedade, causando impactos nas relações humanas e organizacionais, pelo fato de integrar a este processo os indivíduos, empresas, dispositivos, redes, computação distribuída[63], inteligência artificial[64] e internet das coisas - *IoT*[65], sem as barreiras do tempo e de limitações geográficas.

Contudo, para estar em sintonia com os objetivos pretendidos na abordagem do presente

---

[63] Francisco Andrade assim refere-se à expressão: "a computação em nuvem ou"*Cloud Computing*" , é uma das ferrramentas que vem a justificar o quanto se torna mais difícil nos dias atuais assegurar os direitos ao apagamento de dados e ao esquecimento. Trata-se de uma modalidade de prestação de seviços, a partir de servidores internos ou externos que possibilita um acesso ubíquo a uma gama de serviços e de recursos da informática". ANDRADE, Francisco. Comunicações Eletrónicas e Direitos Humanos: O perigo do "*Homo Conectus*." Disponível em: <https://repositorium.sdum.uminho.pt/> Acessado em: 23 de mar de 2020.

[64] A expressão "Inteligência Artificial" refere-se à habilidade de um sistema de interpretar corretamente dados externos, aprender a partir desses dados e usar o aprendizado para alcançar objetivos e tarefas específicos por meio da adaptação flexível. Nesse sentido, ela difere de conceitos como "internet das coisas" ou "*big data*". STEIBEL, Fabro; VICENTE, Victor Freitas; DE JESUS, Diego. Possibilidades e potenciais da utilização da Inteligência Artificial. In: Inteligência artificial e Direito : ética, regulação e responsabilidade. Coordenação Ana Frazão e Caitlin Mulholland. . 1. ed. em e-book - São Paulo : Thomson Reuters Brasil, 2019.

[65] Também denominada "ambientes inteligentes" - consiste na recolha massiva de dados para disponobilização e troca de dados entre vários sistemas, aparelhos e bases de dados que permite uma fácil monitorização das escolhas e atividades do utilizador, através de sistemas cada vez mais sofisticados, dotados até de capacidades de adaptação e de aprendizagem. E isto pode ser realizado através de vulgares dispositivos dotados de capacidade computacional (e.g., ecrãs, câmaras de vídeo, acelerômetros, PDAs), o que nos obriga aum repensar da bordagem das questões relacionadas com a transdparência dos sistemas, o consentimento dos utilizadores e as finmalidades da recolha de dados. ANDRADE, Francisco; COSTA, Ângelo; NOVAIS, Paulo. Privacidade e Proteção de Dados nos Cuidados de Saúde de Idosos. In: Memorias Del XV Congresso Ibero-Americano de Derecho e Informatica. Buenos Aires, elDial.com, 2011.

trabalho, e tendo em vista a amplitude dos conceitos abarcados pela tecnologia da informação com os seus desdobramentos, limitar-se-á o estudo a alguns conceitos trazidos pela LGPD, e pelo RGPD, especificamente aqueles a serem observados pelos Tribunais de Contas do Brasil e de Portugal, sem pretender esgotar seu detalhamento ou explicação.

Destarte, conforme previsto no Art. 4° do RGPD e no Art. 5° da LGPD, pela sua relevância, devem os mencionados TC's ter em conta os conceitos ali discriminados quando da aplicação e adequação de seus sistemas normativos e de seus sistemas de informação, em especial: dados pessoais; dado pessoal sensível; dado anonimizado; banco de dados; titular de dados; responsável pelo tratamento; encarregado de proteção de dados; agentes de tratamento - o controlador e o operador; tratamento de dados; anonimização; pseudonimização; consentimento; transferência internacional de dados; uso compartilhado de dados; relatório de impacto à proteção de dados; autoridade nacional de proteção de dados.

Ambas as legislações principiam nos aludidos artigos com a definição de "dados pessoais"[66], e não poderia ser diferente, eis que objetiva o resgate da dignidade dos titulares de dados, bem como dos direitos a ele relativos, tendo entre seus fundamentos o respeito à privacidade; a inviolabilidade da intimidade, da honra e da imagem; a autodeterminação informativa, sem prejuízo de se almejar o desenvolvimento econômico e tecnológico e a inovação. Ademais, a LGPD inclui expressamente no rol de definições do Art. 5° os "dados sensíveis"[67], e o RGPD discrimina separadamente no Art. 4° os dados assim considerados, além de ter-lhes reservado o Art. 9° ao dispor sobre o "tratamento de categorias especiais de dados pessoais".

Segundo Oliveira e Cots[68], "a LGPD adotou, na definição de dados pessoais, o critério expansionista, ou seja, não define apenas como dados pessoais os dados que, imediatamente, identifiquem uma pessoa natural (viés do critério reducionista), como poderia ser informações como o nome, número do CPF, imagem etc, mas abarcou também os dados que tornam a pessoa identificável de

---

[66] De acordo com RGPD, no artigo dedicado às definições, entende-se por: «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular; Por sua vez, a LGPD considera dado pessoal a informação relacionada a pessoa natural identificada ou identificável. Disponível em: <https://guialgpd.com.br/comparativo-entre-lgpd-x-gdpr/>. Acessado em: 04 de jan. de 2020.

[67] Art. 5° Para os fins desta Lei, considera-se:
II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organizaçãoào de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoal natural. Disponível em: <www.planalto.gov.br>. Acessado em: 04 de jan. 2020.

[68] COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais comentada*. 2.ed.rev.atual. e ampl.- São Paulo: Thomson Reuters . Brasil, 2019. p. 71.

forma não imediata ou direta".

A fim de ilustrar e facilitar a compreensão, imagine-se uma reunião composta por 30 participantes (homens e mulheres), na qual fosse colocada uma venda no palestrante e, a partir de um momento estabelecido, a este fossem passadas diversas informações para que adivinhasse de quem se estava falando. Se a primeira informação indicasse ser alguém do sexo feminino, eliminar-se-ia metade das possibilidades. Na informação seguinte, indicar-se-ia que a pessoa tem pele escura, o que levaria à eliminação de mais uma certa quantidade de participantes. Então, percebe-se que na medida em que o palestrante vai sendo alimentado pelas informações, a possibilidade de identificação da pessoa a que se pretende chegar vai se tornando mais precisa e evidente. Verifica-se que o participante não estava identificado, porém tornou-se identificável mediante a conjugação de informações obtidas a partir do local onde acontecia a reunião.

Trazendo a realidade do conceito para os Tribunais de Contas, objeto do presente trabalho, se estas Entidades Públicas dispõem de um banco de dados que, uma vez alimentados ou conjugados, possam identificar uma pessoa, tais dados serão considerados pessoais, ainda que isoladamente não possam identificar o indivíduo. A utilidade deste entedimento presta-se, por exemplo, aos processos de denúncia, ou mesmo de licitações, a fim de evitar procedimentos fraudulentos.

Uma observação a ser feita refere-se ao fato de que os conceitos de dados e de informações mesclam-se na definição de dados pessoais, sendo oportuno distingui-los com mais precisão. O termo "dados" refere-se a uma informação pré-existente, ou seja, antes do seu tratamento. A esse respeito, o inciso I do artigo 4º da LAI define que a informação é composta de dados – tratados ou não – usados para produção ou para transmissão de conhecimentos. É uma definição jurídica suficiente para explicar a proteção de dados.

Acerca deste tema, não se poderia deixar de citar a explicação bastante didática da autoria de Veronese[69], citando Buckland[70], ao afirmar que o conceito de informação possui ambiguidade e, para compreendê-lo, ele o dividiu em quatro aspectos, os quais estão distribuidos em quadrantes, explicitados conforme o quadro a seguir:

	Intangível	**Tangível**
Individualidade	Informação-como-conhecimento.Exemplo:	Informação-como-coisa. Exemplos: dados,

[69] VERONESE, Alexandre. In *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro* [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva coordenação. -- 1. ed. -- São Paulo: Thomson Reuters Brasil, 2019. Parte I, Cap. 14, p. 1.

[70] BUCKLAND, Michael. *Information and information systems*. Westport, CT: Praeger, 1991. p. 6.

	conhecimento	documentos, conhecimento armazenado
Processos	Informação-como processo. Exemplo: o ser humano ao ser informado	Processamento de informação.Exemplos: o processamento de dados, documentos e a engenharia do conhecimento

Quadro 1. Aspectos do conceito de informação. Fonte: Veronese.

No sentido de estabelecer o limiar entre o conceito de "informação" e o conceito de "dados", assim assevera Michael Buckland: *"Dados" (data), como a forma plural da palavra em latim datum, significa "coisas que são dadas" (things that have been given). Ele é, portanto, um termo apto para a classe de informações-como-coisas que não foram ainda processadas (tratadas) de alguma forma. Usualmente, os 'dados' se referem a quaisquer registros armazenados em um computador*[71].

Vista sob este prisma, a informação refere-se aos dados tratados. Conforme salienta Veronese, "*os dados são características dos objetos (documentos) – abstratos ou concretos – que, após a sua classificação (tratamento), dão origem às informações. A altura de uma pessoa, em si mesma, é um dado físico. Porém, uma vez que ela é mensurada, tornasse uma informação. Essa informação pode ser definida com base em vários sistemas de classificação. O sistema internacional de unidades (métrico) é um exemplo de um sistema de mensuração e de classificação. Existem outros sistemas de medidas, como o sistema britânico de unidades. Outro exemplo pode ser retirado do cotidiano. As receitas e os gastos correntes de um indivíduo também são dados – bancários e pessoais, no caso – que podem ser utilizados como informações, para, por exemplo, avaliar a possibilidade de concessão de um crediário. A Lei do Habeas Data (Lei 9.507/1996) se refere ao objeto tutelado por ela de forma ambígua: dados e informações. Ela tem o seu foco dirigido aos bancos de dados públicos e, assim, regula vários direitos, tais como o acesso aos dados e a sua retificação. Apesar da provável confusão, essa diferenciação conceitual não criou problemas efetivos. Não obstante, a precisão dos dois conceitos – agora – se torna mais relevante, uma vez que o acesso e proteção aos dados pessoais se tornam tão ou mais importantes do que a proteção e o acesso à informação"*[72].

E o autor concluiu de forma brilhante sua análise, com a qual compactua-se, nos seguintes

[71] BUCKLAND, Michael. *Information and information systems*. Westport, CT: Praeger, 1991. p. 45.

[72] VERONESE, Alexandre. Em Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva coordenação. São Paulo: Thomson Reuters Brasil, 2019. Parte I, Cap. 14, p. 1,.

termos: *"Essa diferença científica e técnica não é irrelevante. Primeiro porque é muito importante ter clara a necessidade de proteção dos dados pessoais e não somente das informações pessoais. E isso ocorre exatamente em razão do incremento na capacidade computacional. Se a proteção for outorgada somente às informações, um vasto conjunto de dados – não classificados e não tratados – poderão estar desprotegidos. Toda e qualquer mineração de dados primários estaria sem proteção*"[73].

A par disso, observa-se que há dois tipos de questões a serem consideradas em relação aos dados pessoais: a evolução do direito à proteção das informações pessoais para o direito à proteção dos dados pessoais; e a evolução do tratamento dos dados de um ambiente tecnológico restrito em alcance e produtividade para o atual contexto de *Big Data*[74] (megadados ou grandes dados em português). São fatores a serem considerados pelos sistemas de informações das Entidades Públicas e, consequentemente, pelos Tribunais de Contas, na sua atribuição constitucional de fiscalização daquelas Entidades.

Sobre este ponto, sem haver pretensão de alongar-se, é pertinente dedicar-se breves linhas, posto que se constitui numa expressão do princípio da eficiência buscado pelo Poder Público para escorreita execução dos programas de governo, mas, ao mesmo tempo serve de ferramenta de tecnologia eficaz para o combate à corrupção, para a efetividade da transparência dos gastos públicos e o consequente controle interno e externo das entidades a quem compete a fiscalização.

Com efeito, agregar esta inovação tecnológica permite análises e cruzamentos de grandes volumes de dados impossíveis de serem sistematizados tão somente pela capacidade humana, que vão desde o monitoramento da qualidade dos serviços públicos até instrumentos capazes de mensurar a eficácia de controle na administração, o que é de total interesse dos gestores públicos, posto que se os mecanismos internos de controle falham, os externos (Ministérios Públicos e TC's) desempenham seu papel, punindo os responsáveis pela ação ou omissão.

Concretamente, entre tantos procedimentos, as dispensas de licitação ao arrepio das permissões legais, ou mesmo cotações superfaturadas, além da prévia combinação de preços entre empresas participantes de certames licitatórios, bem como a realização de pagamentos fora da ordem cronológica, e a formalização de contratos com fornecedores impedidos, podem ser citadas entre as irregularidades

[73] Ibid.

[74] O termo *Big Data* é utilizado para definir um grande conjunto de ferramentas de TI que permitem a captura, a análise e a catalogação de registros em tempo real. As informações podem ser originadas de diferentes fontes internas e externas, como cadastro de clientes, análises de mercado, redes sociais, dispositivos eletrônicos, processos internos ou mesmo pesquisas em meios offline. A vantagem dessas ferramentas está em centralizar, em um único local, a coleta e a análise desse grande conjunto de registros. A partir disso, as técnicas de estatística e processamento ficam a cargo das máquinas, permitindo que analistas consigam identificar padrões rapidamente e prever tendências com maior precisão. Disponível em: <https://pt.wikipedia.org/wiki/> Acessado em: 20 de fev. de 2020.

facilmente detectadas por meio de ferramentas de *Big Data*.

A título de exemplo, o Estado de São Paulo, no Brasil, utiliza uma ferramenta de *Big Data* denominada *RevelaGov*[75], uma plataforma que transforma dados públicos em informações tratadas, comparadas de forma descomplicada, a fim de permitir que um cidadão possa entender para onde e como está sendo gasto o seu dinheiro pelos órgãos públicos. Em breve síntese, a ferramenta possibilita o cruzamento de dados das despesas dos últimos dez anos de 1.802 órgãos públicos do Estado de São Paulo e, desta forma, permite a verificação de mais de 1 milhão de indícios de irregularidades.

Dando sequência a este tópico, verifica-se que tanto o RGPD quanto a LGPD incluem a anonimização como instrumento de proteção de dados. Dados anônimos são aqueles pertinentes a um titular não passível de ser identificado pelo controlador ou por qualquer outra pessoa, tendo em conta todos os meios e tempo razoavelmente necessários[76].

Ao se pretender chegar à anonimização de dados, deve-se ter como premissa básica o fato de que os dados pessoais tenham sido coletados e tratados de acordo com a legislação aplicável a essa categoria, vale dizer, havendo vício no processo inicial, o controlador não se eximirá de sua responsabilidade pelo período em que os dados eram passíveis de serem associados a uma pessoa identificável ou identificada. Este processo de anonimização pressupõe o desenvolvimento de técnicas por parte da iniciativa privada e agentes de mercado, o que requer a atuação regulatória pelos Estados (no caso, Brasil, Portugal), em seus ordenamentos jurídicos.

Na atualidade, as duas técnicas mais em evidência são a randomização e a generalização de dados, as quais possuem pontos positivos e negativos a serem considerados. A randomização é o conjunto de técnicas que alteram a veracidade dos dados para remover a vinculação a um indivíduo, porém nem sempre tem a capacidade de reduzir as possibilidades de identificação do titular dos dados, pois os dados ainda serão derivados de um único conjunto, mas combinados com outras técnicas poderão assegurar um nível de abstração considerável. A generalização consiste em ampliar ou diluir os atributos dos titulares de dados, mediante a modificação da respectiva escala ou em ordem de magnitude (ex. uma região em vez de uma cidade, um mês em vez de uma semana). Contudo, nem sempre a generalização eliminará por completo a possibilidade de identificaçào, pois requer a adoção de procedimentos

[75] Ferramenta da *startup Gedanken*, de Ribeirão Preto, no Estado de São Paulo, Brasil. A plataforma utiliza técnicas de *Big Data*, estatística avançada e inteligência artificial para monitorar os gastos públicos e fomentar o controle social. Ela mapeou mais de um milhão de indícios de irregularidades em 1,8 mil órgãos municipais do Estado de São Paulo analisando as despesas de 2008 a 2018, como gastos sem licitação acima do limite legal. Disponível em: <https://www.revelagov.com/>. Acessado em: 20 de fev. de 2020.

[76] SOMBRA, Thiago Luís Santos. *Fundamentos da regulação da privacidade e proteção de dados pessoais: pluralismo jurídico e transparência em perspectiva,* São Paulo: Thomson Reuters Brasil, 2019. p. 170.

sofisticados adicionais para evitar a vinculação e a inferência[77]. Restará, portanto, aos desenvolvedores a função de estabelecer os parâmetros a serem adotados mediante a eliminação irreversível de componentes que possam conduzir à identificação dos indivíduos.

Outro mecanismo de proteção de dados pessoais considerado nas supramencionadas legislações protetivas é a pseudonomização. Trata-se de um processo que se presta a disfarçar a identificação de um titular de dados pessoais, por meio da substituição de um atributo que lhe seja exclusivo por outro tipo de registro, conferindo-lhe um maior nível de segurança. Segundo Thiago Sombra, *ao contrário dos que muitos sustentam, dados pseudonimizados são considerados dados pessoais, ou seja, não envolvem um processo de anonimização, na medida em que o controlador ainda tem condições de identificar o titular. Na pseudonimização, o controlador tem informações adicionais capazes de refazer toda a cadeia de identificação até se chegar novamente no titular dos dados*[78].

Tendo por objetivo a coleta de dados adicionais de um mesmo indivíduo sem a necessidade de saber sua identidade, reduzindo-se assim a possibilidade de identificação, a pseudonimização vale-se de três técnicas, quais sejam: a criptografia[79]; a função *hash*[80]; e a tokenização. Na primeira, somente os detentores da chave privada têm a capacidade de acessar os dados e reidentificar os titulares. A segunda técnica é uma modalidade de algoritmo que mapeia dados de comprimento variável a fim de se atingir dados de comprimento fixo. A tokenização é um processo de usar tokens digitais criptográficos para representar a propriedade de um determinado ativo tangível (imóveis, metais preciosos), ou intangível (ações, títulos, fundos, propriedade intelectual, entre outros). Na prática, cada token tem a função de representar uma porcentagem da propriedade daquele ativo.

São vários os fatores a serem considerados para obter-se a eficácia do procedimento de pseudonomização, tais como: o espaço amostral utilizado, a capacidade de rastreamento reverso e vinculação das informações etc. Por este motivo, os pseudônimos a serem utilizados devem ser aleatórios e imprevisíveis e quanto maior o número de caracteres de um dado pseudonimizado mais

---

[77] SOMBRA, Thiago Luís Santos. *Fundamentos da regulação da privacidade e proteção de dados pessoais: pluralismo jurídico e transparência em perspectiva*, São Paulo: Thomson Reuters Brasil, 2019. p. 172.

[78] Ibid., p. 159.

[79] Criptografia é um sistema de algoritmos matemáticos que codificam dados do usuário para que só o destinatário possa ler, ou seja, consiste em camuflar a mensagem a ser transmitida por um meio, que não é totalmente confiável, de maneira que apenas o destinatário consiga entendê-la. Apenas o destinatário e o remetente têm conhecimento de um dado necessário (a chave) para a correta conversão da mensagem. Disponível em: <https://pt.wikipedia.org/wiki/> . Acessado em: 23 de mar. de 2020. < >

[80] É um mecanismo responsável por transformar uma grande quantidade de dados em uma pequena quantidade de informações. As funções *hashes* podem ser usadas em diversas aplicações, uma delas é na autenticação de dados, que é um mecanismo ou serviço usado para verificar a integridade de uma mensagem em transmissão ou um dado estático (armazenado em disco). Disponível em: <https://pt.wikipedia.org/wiki/>. Acessado em: 23 de mar. de 2020.

difícil a probabilidade de identificação. Deverá ser levado em conta que o dado pseudsonimizado ainda é considerado um dado pessoal, o que pode resultar na identificação de um titular por parte do controlador.

Dando continuidade ao conteúdo deste tópico, é pertinente trazer à baila o conceito de banco de dados, o qual consta do inciso IV, do Art. 5° da LGPD, qual seja "*um conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico*", conquanto não seja inovador nem tampouco conste expressamente no rol de definições do Art. 4° do RGPD. Os textos das duas legislações retromencionadas trata de diversas questões relacionadas a banco de dados, notadamente no que se refere à segurança de dados, o que nos leva a limitar a uma análise específica sobre como as Entidades Públicas podem manter seu banco de dados seguros. Com efeito, o Capítulo VII da LGPD é dedicado à **"**segurança e as boas práticas", ao passo que a secção 2 do Capítulo IV do RGPD refere-se à "segurança dos dados pessoais".

Conforme dispõe a LGPD em seu Art. 46 do Capítulo VII, "o*s agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".*

Por sua vez o Art. 32 do Capítulo IV do RGPD, ao tratar do tema sobre segurança do tratamento, assim reporta-se: "*tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado.* E prossegue delineando quatro características a serem contempladas, a saber: *a pseudonimização e a cifragem dos dados pessoais; a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; e um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.*

Para se alcançar o que impõe os referidos artigos, é fundamental entender como funcionam os diversos tipos de banco de dados, cada um com suas particularidades e aplicabilidades diferentes, os quais estão divididos em duas categorias: modelos relacionais e modelos não relacionais[81]. Sem pretender aprofundar-se neste particular, podem ser citados: o SQL, um modelo relacional que estrutura

[81] ELMASRI, Ramez; NAVATHE, Shamkant B. *Sistemas de banco de dados*. 7. ed. São Paulo: Addison Wesley, 2018. p. 37-43.

os dados em forma de tabela; o NoSQL, modelo não relacional onde os dados são estruturados de forma horizontal; o MySQL, um software livre, ou seja, de código aberto, que consiste num sistema de gerenciamento de banco de dados relacional, onde diversos usuários gerenciam e criam vários bancos de dados, sendo muito recomendado para projetos com *e-commerce*, por exemplo; o SQL Server, sistema de gerenciamento de banco de dados da Microsoft**,** o qual requer licença específica para ser operado e tem a limitação de apenas rodar sistemas operacionais Windows; e o Postgre SQL, um dos sistemas de banco de dados mais robustos, de alta estabilidade e baixo custo de manutenção, o qual é capaz de suportar um enorme volume de dados, sendo por este motivo usado pela Apple, Nasa e Skype[82].

Ademais devem ser consideradas as características de segurança discriminadas na LGPD e RGPD: a confidencialidade (informações acessíveis apenas a quem seja autorizado); a disponibilidade (informações sempre acessíveis a quem puder acessá-las) e integridade (informações fidedignas e autênticas). Associadas a elas estão as boas práticas, as quais podem ser, por exemplo: o limite do acesso à base dados, evitando o acesso idevido e o consequente vazamento de dados; a limitação dos privilégios de alguns usuários, a exemplo da definição de perfis para técnicos que atuam na àrea de desenvolvimento e outros na área de produção; identificar os dados sensíveis e os dados críticos, por meio do mapeamento e anáise de risco; não utilizar a mesma base de dados para testes ao desenvolver uma nova aplicação, evitando assim, que dados sensíveis sejam expostos em uma aplicação que ainda está em fase de testes[83].

Vale salientar ainda que o § 1° do Art. 46 da LGPD atribui à autoridade nacional a faculdade de dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei. E, neste ponto, abre-se um parêntese para discorrer breves linhas sobre a figura da Autoridade Nacional de Proteção de Dados.

Diferentemente do RGPD, que previu desde sua aprovação uma Autoridade Europeia para Proteção de Dados, bem como uma Autoridade de Controlo para cada Estado-Membro (Capítulo VI), além de um Comitê Europeu para a Proteção de Dados (Secção 3, do Capítulo VII), a criação da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD) pela LGPD foi objeto de veto presidencial, postergando-se, com isso,

[82] Qual SGBD se adapta melhor ao seu projeto? Disponível em: <https://meunegocio.uol.com.br/academia/tecnologia/mysql-x-sql-server-x-mongodb-x-postgres--qual-banco-de-dados-escolher.html#rmcl>. Acessado< em: 15 de jun. de 2020.

[83] SETZER, Valdemar W.; SILVA, Flávio Soares Corrêa da. Banco de dados: Aprenda o que são, melhore seu conhecimento, construa os seus. São Paulo: Edgard Blücher, 2005. p. 48.

as respectivas definições, as quais foram introduzidas pelas alterações promovidas pela lei n° 13.853, de 8 de julho de 2019, nos termos do Art. 55-A[84], do Capítulo IX, com autonomia técnica e decisória, conforme Art. 55-B, e atribuições exaustivamente discriminadas, notadamente no Art. 55-J.

O que há de ser observado, em síntese, pelas Entidades Públicas e, portanto, pelos TC's, em relação à atuação destas autoridades de proteção de dados pessoais, é o estabelecimento de normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais, a emissão de parecer técnico complementar para garantir o cumprimento da lei de proteção de dados pessoais, bem como o atendimento às solicitações por elas veiculadas, quais sejam: realização de tratamento de dados pessoais; informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado. Isto porque, a autoridade nacional foi concebida pelo legislador por diversos fatores, mas o principal deles foi a necessidade da atuação de um órgão específico, científica e tecnicamente habilitado, que pudesse atuar com isenção e levando em conta as especificidades inerentes ao tratamento de dados pessoais e sua importância para titulares e controladores[85].

Na sequência dos conceitos ora estudados, é relevante a expressão "tratamento de dados pessoais", a qual tanto a LGPD (inciso X, do Art. 5°)[86] quanto o RGPD (n° 2, do Art. 4°)[87] a definem com precisão e clareza, ressaltando-se apenas que o rol descrito é meramente exemplificativo. Saliente-se que as hipóteses ali elencadas não são cumulativas, vale dizer, uma única atividade descrita é suficiente para o seu enquadramento no conceito de tratamento. Desta forma, o simples fato de armazenar dados pessoais sem utilizá-los constitui tratamento de dados.

No Capítulo II da LGPD estão as principais regras a serem observadas para o tratamento de dados, aí incluídos os requisitos ou bases legais, o consentimento, o tratamento de dados pessoais sensíveis, o tratamento de dados pessoais de crianças e adolescentes, o término e a eliminação de dados pessoais após o tratamento. A seu turno, o RGPD estabelece as regras acerca do tratamento de dados

---

[84] Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. Disponível em:: <www.planalto.gov.br/legislação>. Acessado em: 28 de mar. de 2020.

[85] COTS, Márcio; OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Pessoais comentada. 2.ed.rev.atual. e ampl.- São Paulo: Thomson Reuters . Brasil, 2019. p. 151-152. .

[86] X - tratamento: toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Disponível em: <www.planalto.gov.br>. Acessado em: 28 de mar. de 2020.

[87] 2) «Tratamento», uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição. Disponível em: <https://eur-lex.europa.eu/>. Acessado em: 29 de mar. de 2020.

pessoais sob o título de "princípios", principiando no Art. 5° e finalizando no Art. 11° do Capítulo II. As disposições ali constantes abrangem: os princípios; a licitude, as condições aplicáveis ao consentimento em geral e ao consentimento de crianças em relação aos serviços da sociedade da informação; o tratamento de categorias especiais (saúde, por exemplo); o tratamento de dados pessoais relacionados com condenações pessoais e infracções; e o tratamento que não exige identificação.

Não é objetivo deste trabalho aprofundar-se neste tema, porém não se poderia deixar de fazer referência ao "atendimento de uma finalidade pública", à "persecução do interesse público"[88] e à "execução, pelo ente público, de suas competências legais ou cumprimento de suas atribuições" pelos quais se devem pautar as atividades de tratamento de dados pelas Entidades Públicas. Ora, o atendimento de uma finalidade pública somente é possível se o interesse a ser perquerido for igualmente público, ou seja, há uma interdependência dos dois pressupostos.

No que toca à execução das competências ou atribuições legais, cada ente público possui sua investidura legal para praticar o ato e exercer uma função, pois recebe uma parcela da soberania do Estado para funções jurídicas, de ordem pública e administrativa, que lhe são cometidas por lei.[89] Destarte, admite-se o tratamento de dados pela entidade pública para execução de seu propósito de existir. Por outro lado, se o tratamento de dados ocorrer fora da competência ou atribuição legal do órgão público, será eivado de ilegalidade. Devido a isto, a legislação protetiva de dados estabelece, entre outros requisitos para o tratamento de dados: que a entidade pública publique de forma clara e precisa, de preferência em seu sítio eletrônico, informações relativas ao tratamento, como a previsão legal, a finalidade, os procedimentos e práticas utilizadas no tratamento; e que seja indicado um encarregado pelo tratamento de dados pessoais.

Além disso, o Art. 30° do RGPD consagra uma obrigação que não existia na Diretiva 95/46/CE, e que é uma das manifestações do dever de *accountability*[90], qual seja, "*a obrigação de proceder ao registro de tratamento de dados pessoais, a qual está referida já no n° 2 do Art. 5°, ao estabelecer que "o responsável pelo tratamento é responsável pelo cumprimento do disposto no n° 1 (princípios relativos ao tratamento de dados pessoais) e tem de poder comprová-lo (<responsabilidade>). É esta comprovação do cumprimento da lei que a obrigação de registro de*

---

[88] Cf. Bandeira de Melo, o *"interesse público deve ser conceituado como o interesse resultante do conjunto de inbteresses que os indivíduos pessoalmente têm quando considerados em sua qualidade de membros da sociedade e pelos simples fato de o serem".* BANDEIRA DE MELLO, Celso Antônio. Curso de direito administrativo. 19. ed. São Paulo. Malheiros, 2005. p.51.

[89] CAVALCANTI, Themistóclis Brandão. Teoria dos atos administrativos. São Paulo: ed. RT. 1973, p. 67

[90] Cf. Thiago Sombra, "Sob a perspectiva do controle, a accountability diz respeito à capacidade que os cidadãos têm de impor e cobrar a imposição de sanções aos seus representantes, o que inclui a prestação de contas de suas atividades". SOMBRA, Thiago Luís Santos. Fundamentos da regulação da privacidade e proteção de dados pessoais: pluralismo jurídico e transparência em perspectiva, São Paulo: Thomson ReutersBrasil, 2019. p. 209.

atividades de tratamento visa satisfazer"[91].

A LGPD e o RGPD apresenta em seus textos algumas pessoas envolvidas com o tratamento de dados pessoais, já referidas no corpo deste trabalho, as quais ocupam posições e atribuições que não se confundem e que são essenciais ao cumprimento daquelas normas. Para os objetivos propostos, importa comentar apenas aquelas que os retrocitados diplomas normativos impõem a obrigatoriedade de sua existência no âmbito dos Tribunais de Contas, bem como daquelas as quais, ainda que indiretamente, mantenham com estas Entidades atividades que exijam o conhecimento dos requisitos para o tratamento de dados pessoais. Trata-se das seguintes figuras: do titular dos dados pessoais; dos agentes de tratamento – controlador e operador; do encarregado de proteção de dados; do responsável pelo tratamento; do subcontratante; e do terceiro. Vale salientar que nem todas estão presentes nas duas legislações.

As regras atinentes ao titular dos dados pessoais estão dispostas no Capítulo III de ambas as legislações, capítulo dedicado aos direitos do titular, se bem que a LGPD a ele refere-se no inciso V do Art. 5° ao defini-lo como sendo *"pessoa natural a quem se referem os dados pessoais que são objeto de tratamento"*. Certo é, contudo, que as Entidades Públicas deverão estar atentas às disposições atinentes aos direitos que são assegurados ao titular dos dados e, por conseguinte, os agentes de tratamento e demais pessoas que os represente. Dado que o rol de direitos conferidos ao titular de dados são extensos, a análise concentrar-se-á apenas em alguns a serem observados pelos Tribunais de Contas, sendo recomendada a leitura na íntegra dos demais direitos elencados nas normas sobreditas.

Da própria definição legal, infere-se que toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, intimidade e de privacidade, o que é reforçado pelo Art. 17° da LGPD, e pelo Art. 12° do RGPD, em observância às limitações impostas pelo princípio da transparência das informações, das comunicações e das regras para o exercício dos direitos dos titulares de dados e dos demais princípios relativos ao tratamento de dados pessoais (limitação da conservação, licitude, lealdade, minimização de dados, confidencialidade, entre outros).

As legislações protetivas dos dados pessoais reconhecem que a titularidade destes dados sempre será de pessoa natural, não podendo ser objeto de cessão ou transferência, à exceção dos casos previstos em lei. Esta assertiva tem fundamento no próprio CC. do Brasil, cujo Art. 11, assim prescreve: "com exceção dos casos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária". Neste norte, os negócios jurídicos, ou mesmo o uso de informações pela Administração Pública, os quais contemplem a cessão ou transferência de dados

[91] FAZENDEIRO, Ana. Regulamento geral sobre proteção de dados. Coimbra: Almedina. 2018. p. 23,.

pessoais, ou que limitem seu exercício, deverão ser considerados nulos. Depreende-se, portanto, não haver a possibilidade de renúncia da titularidade sobre os dados pessoais.

Um outro ponto a ser considerado na definição do titular de dados, segundo Roberta Mauro, é que a opção legislativa, manifestada no caput do art. 17 da LGPD, de tratar a pessoa física a quem os dados se vinculam como seu titular, "[...] denota a intenção de refletir que o exercício do direito ali descrito se dará de modo direto e imediato, empregando-se termo que corresponde ao gênero do qual a propriedade é espécie. Tal passagem da lei evidencia, ainda, a preocupação em demonstrar que a tutela ali conferida tem dupla natureza, restando contemplados os aspectos patrimoniais decorrentes da disposição dos dados – atribuída ao seu titular – e os extrapatrimoniais. Portanto, o referido dispositivo legal serve de exemplo da constatação, por parte do legislador, de que a distinção mais relevante para o direito civil, hoje, não é a que aparta direitos reais e obrigações, mas sim as que separam as relações jurídicas absolutas das relativas e as patrimoniais daquelas extrapatrimoniais"[92].

É cediço que os direitos dos titulares estão relacionados ao tratamento de dados e relação jurídica entre ele e o responsável (ou controlador), ou seja, não restringe direitos previstos em outras legislações quando incidentes sobre a totalidade ou parte da referida relação. Acerca disso, Cots salienta que "[...] *o exercício de tais direitos é realizado mediante requisição, ou seja, não se trata de pedido ou solicitação, não podendo o responsável se opor, salvo nos casos previstos na LGPD"*[93].

O titular tem direito a ter a confirmação da existência de tratamento, acesso aos dados tratados e os corrigir, quando incompletos, inexatos e desatualizados. Este é um dos motivos pelos quais o RGPD diferencia os requisitos a serem cumpridos quando os dados pessoais forem recolhidos junto ao titular daqueles dados pessoais não recolhidos junto ao titular, garantindo, assim, o exercício do direito de acesso. Tais direitos são vinculados aos princípios da transparência, livre acesso e qualidade dos dados.

É importante ressaltar que se for constatado pelo titular que há dados desnecessários ou excessivos, bem como, se o tratamento estiver se dando em desconformidade com a finalidade prevista, o titular poderá exigir a anonimização, bloqueio ou eliminação de dados, situação em que deverá especificar qual dessas ações deverá ser tomada. A esse respeito, Cots alerta para o fato de que "o titular não possui conhecimento técnico para tomar essa decisão, cabendo ao controlador adotar a medida que afaste a incidência da LGPD, mas, por outro lado, que atenda aos seus interesses (por exemplo, a anonimização pode ser mais benéfica do que a eliminação, se houver interesse em dados estatísticos)"[94].

---

[92] MAURO, Roberta. Em *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro* [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva coordenação. -- 1. ed. -- São Paulo : Thomson Reuters Brasil, 2019. Parte I, Cap. 5, p. 5.

[93] COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais comentada*. 2.ed.rev.atual. e ampl.- São Paulo: Thomson Reuters . Brasil, 2019. p. 124-125,

[94] Ibid.

Uma vez delineada a figura do titular de dados pessoais, tratar-se-á de explicitar uma outra inplementada pelas duas legislações de proteção de dados pessoais: o Encarregado de Proteção de Dados - EPD. A LGPD define o "encarregado" no inciso VIII do Art. 5°, nos seguintes termos: "pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares de dados e a ANPD" . Contudo, detalha as suas atribuições e as responsabilidades civil e penal apenas na Secção II, do Capítulo VI, o qual se intitula "agentes de tratamento de dados pessoais". Diferentemente, o RGPD não o elenca no rol de definições, porém a ele dedica toda a secção 4, do Capítulo IV (Responsável pelo tratamento e subcontratante), estabelecendo as regras relativas a sua designação (Art. 37); a sua posição em relação aos demais envolvidos no tratamento de dados pessoais e os titulares de dados (Art. 38°); e as funções a serem por ele exercidas, entre as quais a de cooperação com a autoridade de controle (Art. 39°).

Em relação aos Organismos Públicos ou Entidades Públicas e, portanto, os Tribunais de Contas, o RGPD impõe ao responsável pelo tratamento a designação de um encarregado sempre que o tratamento for efetuado por uma autoridade ou organismo público, excetuando os tribunais no exercício da sua função jurisdicional (alínea "a", n°1 do Art. 37°), ao passo que a LGPD impõe este dever ao controlador (Art. 41), sendo ao encarregado atribuida, entre outras funções, a de orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados (inciso III, do § 2°, do Art. 41°). Neste aspecto, o TC. de Portugal já designou o seu encarregado de proteção de dados pessoais, bem como vem delineando o seu estatuto (documento), detalhando as suas atribuições, enquanto os TC's do Brasil ainda se encontram em fase de estudo para o cumprimento desta regra.

O entendimento prevalente no Tribunal de Contas de Portugal é de que uma vez designado de forma voluntária (caso aplicável ao Tribunal no exercício de sua função jurisdicional, conforme parte final da alínea "a", do n° 1 do Art. 37° do RGPD), o EPD assume todas as operações de tratamento realizadas pelo responsável pelo tratamento ou pelo subcontratante (se for o caso), sendo aplicável a sua nomeação, posição e funções o disposto nos Artigos 37° a 39° do RGPD. Desta forma, as funções do EDP abrangem todas as operações de tratamento de dados pessoais, tal como se encontra definido no n°. 2° do Art. 4° do RGPD, incluindo aquelas que não digam respeito ao desempenho de funções públicas ou oficiais, quais sejam, a gestão de base de dados de trabalhadores ou de fornecedores. Seguindo as orientações do GT29[95], o principal *múnus* do EPD será o de permitir e favorecer o cumprimento do RGPD, que se traduz no "desempenho de um papel determinante na promoção de uma cultura de

[95] GT29 – Grupo de Trabalho instituído ao abrigo do Art. 29° da Diretiva 95/46/CE (GT29), órgão consultivo europeu independente em matéria de proteção de dados e privacidade. Disponível em: <www.tcontas.pt/geral>. Acessado em:10 de dez. de 2019.

proteção de dados no seio da organização e contribui para dar cumprimento aos elementos essenciais do RGPD, tais como os princípios do tratamento de dados, os direitos dod titulares de dados , a proteção de dados desde a concepção e por defeito, os registros das atividades de tratamento, a segurança do tratamento e a notificação e comunicação de violações de dados".

Cabe ressaltar que na Diretiva 95/46/CE não havia a previsão da figura do encarregado de proteção de dados, embora já estivesse prevista na legislação de vários países europeus, a exemplo da Lei Federal Alemã, para a qual a pessoa a quem forem atribuídas as funções de encarregado deve ser um profissional altamente qualificado, sendo protegido em situação de despedimento, exceto em caso de incumprimento grave dos seus deveres, conforme expõe Ana Fazendeiro[96]. Tal exigência de qualificação profissional não foi seguida pelo RGPD, contudo não impede aos Organismos Públicos de assim o fazerem para melhor atender as suas necessidades.

Nos parágrafos anteriores, foi feita referência a quatro figuras envolvidas no tratamento de dados pessoais: o responsável pelo tratamento; o subcontratante; o controlador e o operador. Quanto aos termos empregados, a LGPD e o RGPD não convergem, conquanto ao defini-las haja uma similaridade conceitual e de atribuições, não tendo implicações significativas para os Tribunais de Contas.

Com efeito, o "Responsável pelo tratamento", constante do n° 7 do Art. 4° do RGPD, é a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro. É um conceito mais amplo se comparado ao de "Controlador", do inciso VI, do Art. 5° da LGPD, qual seja, "a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais". Observa-se que o responsável pelo tratamento determina as finalidades e os meios de tratamento de dados pessoais, e ao controlador compete as decisões referentes ao tratamento de dados pessoais. Ambos não realizam o tratamento de dados, apenas decidem, determinam as finalidades e os meios de tratamento no âmbito das respectivas organizações públicas ou privadas. A execução do tratamento, ou seja, o tratamento em si, à luz da LGPD cabe ao "operador", que é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, consoante o inciso VII do Art. 5°.

Sob a égide do RGPD, é o "subcontratante", uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trata os dados pessoais por conta do responsável pelo

[96] FAZENDEIRO, Ana. Regulamento geral sobre proteção de dados. Coimbra: Almedina. 2018. p. 19.

tratamento destes, segundo o disposto no n° 8 do Art. 4°. Vale frisar, ainda, que o RGPD, no n° 10 do Art. 4°, autoriza um outro personagem, não previsto na LGPD, a tatar os dados, a figura do "terceiro", qual seja, a pessoa singular ou coletiva, a autoridade pública, o serviço ou organismo que não seja o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar os dados pessoais.

Conquanto todas as figuras delineadas acima não se apliquem em sua inteireza à estrutura orgânica dos Tribunais de Contas, convém clarificar com um exemplo prático da autoria de Márcio Cots como funciona essa engrenagem: uma empresa X, fabricante de artigos esportivos, deseja ter um *site* para a venda de seus produtos diretamente aos consumidores, mas, como o comércio virtual não é sua atividade principal, deseja delegar algumas delas a prestadores de serviço. Assim, contrata uma plataforma virtual completa com a empresa A; a gestão e meio de pagamento com a empresa B; a gestão da logística com a empresa C; e a gestão do *marketing* e propaganda com a empresa D. Ao receber um pedido, os dados pessoais do usuário primeiro são captados pela plataforma (empresa A), depois segue para o meio de pagamento (empresa B) ao mesmo tempo em que é incorporada ao banco de dados da empresa Y. Em seguida, os dados pessoais seguem para a empresa D, com a determinação de que realize a entrega do produto, ao mesmo tempo em que são encaminhados à empresa E, para inclusão no *mailing*[97] e demais atividades de divulgação. A conclusão a que se chega é de que todas as empresas mencionadas terão acesso aos dados pessoais do usuário do *site,* mas apenas a empresa X se encaixa na figura do controlador, o qual cumpre uma função específica no processo de tratamento[98].

Dando encadeamento lógico aos conceitos até então abordados, surge um questionamento acerca da legitimação dos tratamentos de dados pessoais, sob pena de serem os agentes de tratamento e demais envolvidos com a proteção de dados acusados de apoderarem-se indevidamente de um bem que não os pertence e deles dispor sem reservas. À limitação a eventual ação neste sentido, o RGPD e a LGPD apresentam um conceito estreitamente vinculado ao titular dos dados pessoais, qual seja o "consentimento". De acordo com o n° 11 do Art. 4° do RGPD, o consentimento do titular dos dados consiste numa manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento. A seu turno, o inciso XII do Art. 5° da LGPD define-o como uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados

[97] Palavra originária do inglês, que tem como significado correio - o ato de enviar uma correspondência a alguém. Insere-se no conceito de banco de dados para serem utilizados em marketing direto, tais como mala direta, telemarketing e correio eletrônico. Disponível em: <http://periodicos.ufpb.br/ojs2/index.php/tematica> Acessado em: 30 de mar. de 2020.

[98] COTS, Márcio; OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Pessoais comentada. 2.ed.rev.atual. e ampl.- São Paulo: Thomson Reuters . Brasil, 2019. p. 125.

pessoais para uma finalidade determinada.

Ao comparar-se os qualificadores acrescidos ao consentimento pela LGPD com o modelo regulado pelo RGPD, verifica-se uma perfeita identificação, daí dizer-se que a legislação brasileira pode ser praticamente considerada como um transplante legal desta última[99]. O quadro comparativo abaixo ilustra de forma didática as similitudes entre as duas legislações:

De acordo com a LGPD, o consentimento em geral deve ser:	De acordo com o RGPD, o consentimento em geral deve ser:
* Prévio * Livre, Informado, Inequívoco * Para uma finalidade determinada * Manifestado por escrito ou outra forma de expressar a vontade do titular * Em se tratando de dados sensíveis deve ser específico e em destaque * Possível de revogação a qualquer tempo	* Prévio * Livre, Informado, Inequívoco * Para uma finalidade determinada * Manifestado explicitamente por declaração ou ato positivo * Em se tratando de dados sensíveis deve ser específico e em destaque * Possível de revogação a qualquer tempo

Quadro 2. Aspectos do conceito de Consentimento Fonte: produzido pelo autor.

É pertinente trazer à baila um trecho do "Considerando 50" do RGPD, o qual expõe com clareza quando o titular dos dados dá o seu consentimento ou quando o tratamento se baseia em disposições do direito da União ou de um Estado-Membro ou caso o tratamento seja necessário para o exercício de funções de interesse público ou o exercício de autoridade pública da qual está investido o responsável pelo tratamento, a saber: "Se o tratamento for necessário para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, o direito da União ou dos Estados-Membros pode determinar e definir as tarefas e finalidades para as quais o tratamento posterior deverá ser considerado compatível e lícito. As operações de tratamento posterior para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, deverão ser consideradas tratamento lícito compatível. O fundamento jurídico previsto no direito da União ou dos Estados-Membros para o tratamento dos dados pessoais pode igualmente servir de fundamento jurídico para o tratamento posterior.

E segue o retromencionado Considerando 50: [...] Caso o titular dos dados tenha dado o seu

[99] MATTEI, Ugo, Efficiency in legal transplants: An essay in Comparative Law and Economics, Intyernational Review of Law and Economics, 1994. v. 14, p. 3-19.

consentimento ou o tratamento se baseie em disposições do direito da União ou de um Estado-Membro que constituam uma medida necessária e proporcionada, numa sociedade democrática, para salvaguardar, em especial, os importantes objetivos de interesse público geral, o responsável pelo tratamento deverá ser autorizado a proceder ao tratamento posterior dos dados pessoais, independentemente da compatibilidade das finalidades. Em todo o caso, deverá ser garantida a aplicação dos princípios enunciados pelo presente regulamento e, em particular, a obrigação de informar o titular dos dados sobre essas outras finalidades e sobre os seus direitos, incluindo o direito de se opor. A indicação pelo responsável pelo tratamento de eventuais atos criminosos ou ameaças à segurança pública e a transmissão dos dados pessoais pertinentes, em casos individuais ou em vários casos relativos ao mesmo: ato criminoso ou ameaça à segurança pública, a uma autoridade competente deverão ser consideradas como sendo do interesse legítimo do responsável pelo tratamento. Todavia, deverá ser proibido proceder à transmissão no interesse legítimo do responsável pelo tratamento ou ao tratamento posterior de dados pessoais se a operação não for compatível com alguma obrigação legal profissional ou outra obrigação vinculativa de confidencialidade.

Por conseguinte, as Entidades da Administração Pública deverão levar em conta estas orientações, notadamente também nas hipóteses do tratamento de dados pessoais de acesso público sem a coleta do Consentimento, posto que o dado de acesso público que identifica ou torna identificável uma pessoa continua sendo dado pessoal e, em consequência, protegido pela LGPD e pelo RGPD.

Conforme comentado neste tópico, o Poder Público poderá realizar tratamento de dados em determinadas circunstâncias, as quais incluem a comunicação e compartilhamento de dados com terceiros ou mesmo entre Entidades da Administração Pública no exercício de suas competências asseguradas por lei. Em relação a isto, as legislações de proteção de dados estabelecem regras específicas a serem observadas, em virtude do aumento crescente da inportância da informação na economia, e a consequente pressão que as Entidades Públicas, seus dirigentes, funcionários tenham que enfrentar para a transferência de dados.

No tocante a isto, o Art. 26 da LGPD prescreve que o uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais, ao passo que o § 1° do mesmo artigo veda ao Poder Público a transferência de dados pessoais a entidades privadas, exceto nos casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na LAI; nos casos em que os dados forem acessíveis publicamente; quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentros congêneres; ou na hipótese de a transferência dos dados

objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, vedado o tratamento para ouitras finalidades.

Em se tratando da comunicação ou do uso compartilhado de dados pessoais de pessoa jurídica de direito público (Administração Pública, por exemplo) a pessoa de direito privado, será obrigatória a informação autoridade nacional e dependerá de consentimento do titular, exceto nas exceções especificadas no parágrafo anterior; nas hipóteses de dispensa de consentimento (interesse legítimo ou tutela da saúde, por exemplo); e nos casos de uso compartilhado de dados em que será dada publicidade nos termos do inciso I do caput do art. 23[100], da LGPD.

Diferentemente, o RGPD não faz distinção entre os setores público e privado, ou seja, aplica-se as regras de uso compartilhado de dados indistintamente as duas naturezas de pessoas jurídicas. É o que se depreende da Lei n° 58/2019[101], de 8 de agosto de 2019, a qual assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Assim, nos termos do n° 1 do Art. 2°, a lei aplica-se aos tratamentos de dados pessoais realizados no território nacional, independentemente da natureza pública ou privada do responsável pelo tratamento ou do subcontratante, mesmo que o tratamento de dados pessoais seja efetuado em cumprimento de obrigações legais ou no âmbito da prossecução de missões de interesse público, aplicando-se todas as exclusões previstas no artigo 2.º do RGPD.

Ainda em relação à comunicação ou ao compartilhamento de dados, há de ser observada algumas regras contidas na retromencionada Lei n° 58/2019[102], de 8 de agosto de 2019, no tocante ao dever de segredo[103] (Art. 20°), relativo aos direitos de informação e de acesso aos dados pessoais previstos nos artigos 13° a 15° do RGPD e também o disposto no Art. 22°, relativo às transferências de

---

[100] Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que: I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos. Disponível em: <www.dre.pt/pesquisa> Acessado em: 22 de dez. de 2019.

[101] Diário da República n.º 151/2019, Série I de 2019-08-08. Disponível em: <www.dre.pt/pesquisa>. Acessado em: 22 de dez. de 2019.

[102] Ibid.

[103] Artigo 20.º

Dever de segredo

1 - Os direitos de informação e de acesso a dados pessoais previstos nos artigos 13.º a 15.º do RGPD não podem ser exercidos quando a lei imponha ao responsável pelo tratamento ou ao subcontratante um dever de segredo que seja oponível ao próprio titular dos dados.

2 - O titular dos dados pode solicitar à CNPD a emissão de parecer quanto à oponibilidade do dever de segredo, sem prejuízo do disposto no Capítulo VII. Disponível em: <www.dre.pt/pesquisa> Acessado em: 22 de dez. de 2019.

dados[104] e no Art. 23°, o qual dispõe sobre o tratamento de dados pessoais por entidades públicas para finalidades diferentes[105], caso em que, além do estabelecido no n° 1 deste artigo, deve ser objeto de protocolo que estabeleça as responsabilidades de cada entidade interveniente, quer no ato de transmissão, quer em outros tratamentos a efetuar.

Ressalte-se, contudo, que afora as hipóteses legalmente permitidas às Entidades Públicas no uso de suas competências para execução de suas atividades fins ou específicas, a exemplo das fiscalizações, auditorias realizadas pelos Tribunais de Contas, o cruzamento de dados entre Tribunais de Contas e Ministério Público ou Órgão do Poder Judiciário, entre outros, não está afastada a obrigatoriedade de consentimento do titular para a comunicação ou compartilhamento de seus dados.

É imprescíndível que as ações das Entidades Públicas estejam em sintonia com os princípios e regras das legislações de proteção de dados pessoais, principalmente pelo fato de que alguns dados são acessíveis publicamente e, assim, permite o compartilhamento ou o acesso, inclusive por terceiros. Para se ter ideia da importância desta assertiva, recorramos a um exemplo hipotético, da autoria de Cots e Oliveira[106]. Imagine-se uma Junta Comercial, que dá ampla publicidade aos dados que registra, mas cujo acesso depende de procedimentos específicos e de certa forma trabalhosos par ser feito em larga escala, pois se utiliza de *login*, senha e *captcha*[107]. Assim, o banco de dados da referida Junta Comercial possui informações valiosas para o mercado, e poder receber os dados sem as barreiras de autenticação, como poderia ocorrer no caso de compartilhamento ou comunicação do banco, seria certamente um ativo importante para inúmeras empresas. Desta forma, a Junta comercial poderia escolher com quem compartilhar seu banco de dados. O mesmo raciocínio poderia ser aplicável ao banco de dados do Poder

---

[104] Artigo 22.º

Transferências de dados

As transferências de dados para países terceiros à União Europeia ou organizações internacionais, efetuadas no cumprimento de obrigações legais, por entidades públicas no exercício de poderes de autoridade, são consideradas de interesse público para efeitos do disposto no n.º 4 do artigo 49.º do RGPD. Diário da República n.º 151/2019, Série I de 2019-08-08. Disponível em: <www.dre.pt/pesquisa>. Acessado em: 22 de dez. de 2019.

[105] Artigo 23.º

Tratamento de dados pessoais por entidades públicas para finalidades diferentes

1 - O tratamento de dados pessoais por entidades públicas para finalidades diferentes das determinadas pela recolha tem natureza excecional e deve ser devidamente fundamentado com vista a assegurar a prossecução do interesse público que de outra forma não possa ser acautelado, nos termos da alínea e) do n.º 1, do n.º 4 do artigo 6.º e da alínea g) do n.º 2 do artigo 9.º do RGPD. Diário da República n.º 151/2019, Série I de 2019-08-08. Disponível em: <www.dre.pt/pesquisa>. Acessado em: 22 de dez. de 2019.

[106] COTS, Márcio; OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Pessoais comentada. 2.ed.rev.atual. e ampl.- São Paulo: Thomson Reuters . Brasil, 2019. p. 149.

[107] CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart - Teste de Turing público completamente automatizado para distinguir entre computadores e pessoas) é um tipo de medida de segurança conhecido como autenticação por desafio e resposta. Disponível em: <https://pt.wikipedia.org/wiki/> . Acessado em: 21 de fev. de 2020.

Judiciário ou órgãos administrativos de determinados programas sociais que exigem certo nível de transparência, entre outros casos. Uma outra hipótese poderia ser o compartilhamento de banco de dados por meio de consulta pública do próprio órgão, mas cuja origem estava sobre o controle de terceiro, por exemplo, banco de dados formado pela Junta Comercial com dados consultados no Tribunal de Justiça e compartilhado, posteriormente, com terceiros.

Por fim, ressalte-se que a autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e compartilhamento de dados pessoais, realizados por quaisquer tipos de controlador ou responsável, incluídos os das Entidades de Direito Público, o que é essencial, porquanto proporciona segurança jurídica a determinadas questões ou dúvidas que venham a ser levantadas no processo de adpatação às legislações de proteção de dados.

Outro procedimento a ser cumprido pelo responsável pelo tratamento de dados ou pelo controlador diz respeito a emissão de um documento ou relatório decorrente da AIPD. Conforme definido no inciso XVII do Art. 5° da LGPD, o relatório de impacto à proteção de dados pessoais (RIPD) é documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. O RGPD, por sua vez, inovou, ao criar, no n° 1 do Art. 35°, a obrigatoriedade de realização de uma AIPD, quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, caso em que o responsável pelo tratamento procede, antes de iniciar o tratamento, a dita avaliação.

Em relação a AIPD, o Tribunal de Contas de Portugal abordou o tema tendo por base o texto "Nova Orientação do Grupo de Trabalho do Art. 29° (GT29) relativa à Avaliação de Impacto Sobre a Proteção de Dados"[108], os quais definem a AIPD, de acordo com o GT29, como "um processo destinado a descrever o tratamento, avaliar a necessidade e proporcionalidade do tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares resultantes do tratamento de dados pessoais, avaliando-os e determinando as medidas para lidar com os mesmos". No dizer de Costa e Ramalho, "trata-se de um mecanismo de gestão de risco dos direitos dos titulares dos dados e não da organização, devendo ser adaptada à realidade de cada organização. Em certos casos, constituirá inclusivamente uma boa prática a divulgação pública da AIPD realizada ou de um sumário com as respetivas conclusões".[109]

O Tribunal de Contas de Portugal e, pode-se dizer, os demais Tribunais de Contas entendem

[108] COSTA, Thiago; RAMALHO, David. *"LEGAL ALERT - Nova Orientação do Grupo de Trabalho do 29.º relativa a Avaliações de Impacto sobre a Proteção de Dados".* Disponível em: <https://www.mlgts.pt/xms/files/v1/Publicacoes>. Acessado em: 22 de fev. 2020.

[109] Ibid.

que as AIPD são instrumenmtos importantes também em matéria de responsabilização, posto que ajudam os responsáveis pelo tratamento a cumprirem os requisitos das respectivas legislações de proteção, além de atestar que foram adotadas medidas adequadas para assegurar a conformidade com aquelas normas. Por este motivo, a AIPD deve ser realizada antes do tratamento e deve ser considerada como um instrumento evolutivo e, por ser o tratamento de dados uma realidade mutável, a avaliação deve ser continuamente realizada para tratamento de dados em curso e reavaliada no prazo máximo de três anos, conforme orientação do GT29.

Entre os critérios a serem considerados para aferir a necessidade de realizar uma AIPD, citados por Costa e Ramalho, incluem-se o tratamento de dados destinados a (i) avaliação e classificação dos titulares, designadamente *profiling*[110] (e.g. uma empresa que define perfis comportamentais baseados na navegação dos utilizadores do seu *website*), (ii) tomadas de decisão automatizadas com efeito jurídico ou análogo, (iii) monitorização sistemática, (iv) tratamento de dados sensíveis, que incluem os dados relativos a comunicações, a localização, a saúde, bem como os dados financeiros e, em certos casos, dados tratados para fins puramente pessoais (como em matéria de serviços de armazenamento na nuvem de informação pessoal ou de apps com registo de informação diária do utilizador), (v) tratamento de dados em grande escala, (vi) tratamentos de dados resultantes de uma interconexão; (vii) tratamento de dados relativos a indivíduos especialmente vulneráveis; (viii) utilização inovadora ou aplicação de soluções tecnológicas ou organizacionais, como seja a combinação do uso de impressões digitais com reconhecimento facial para controlo de acessos; (ix) transferência de dados para países terceiros, (x) ou quando o tratamento impede o titular dos dados de exercerem um direito ou utilizarem um serviço ou contrato[111].

Convém abrir-se espaço para dedicar algumas linhas ao *Profiling,* cuja definição se encontra referenciada em nota de roda-pé. Conforme o considerando 72, o Comitê Europeu para a Proteção de Dados, o qual substitui o Grupo de trabalho do Art. 29, tem a incumbência de emitir orientações no âmbito das operações de tratamento de dados que incluam *profiling*. Salienta Ana Fazendeiro que, embora por princípio, o titular dos dados tenha o direito de não ficar sujeito a decisões baseadas em

[110] RGPD

Art. 4°

Definições

4) «Definição de perfis», qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica,saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações. Cfe. FAZENDEIRO, Ana. *Regulamento geral sobre proteção de dados*. Coimbra: Almedina. 2018. p. 135.

[111] COSTA, Thiago; RAMALHO, David. *"LEGAL ALERT - Nova Orientação do Grupo de Trabalho do 29.º relativa a Avaliações de Impacto sobre a Proteção de Dados".* Disponível em: <https://www.mlgts.pt/xms/files/v1/Publicacoes>. Acessado em: 22 de fev. 2020.

tratamentros automatizados dos dados, aí incluído o *profiling*, estas serão possíveis, nos termos do Art. 22° do RGPD, quando: a) necessárias para a celebração de um contrato ou execução do mesmo entre o titular dos dados e o responsável pelo tratamento; b) autorizadas pela lei de um Estado-Membro; c) existir consentimento explícito do titular. Nos caso previstos em a) e c), "o responsável pelo tratamento deve implementar medidas para salvaguarda dos direitos dos titulares, devendo, no mínimo, ser assegurado o direito do titular de obter intervenção humana, expressar a sua opinião ou mesmo contestar a decisão"[112]. Cabe ressaltar que, mesmo sendo legítimo o tratamento relativo a *profiling*, ainda assim, com base no Art. 21° do RGPD, o titular dos dados tem o direito de oposição, posto que o aludido dispositivo consagra um direito específico de oposição a decisões automatizadas. Vê-se, portanto, que a existência de *profiling* constitui-se num dos motivos pelos quais a realização de avaliações de impacto é obrigatória.

Uma das conclusões a que chegou o TC. de Portugal, considerando os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao trtamento de dados pessoais, foi de que a metodologia de preparação para aplicação do RGPD tem em conta que, no caso de terem sido identificados tratamentos de dados pessoais suscetíveis de gerar riscos elevados para os direitos e liberdades dos titulares dos dados deve proceder-se, para cada tratamento, a uma avaliação de impacto sobre a proteção de dados (AIPD), nos termos do Art. 35° do RGPD[113].

Para finalizar este capítulo, não se poderia deixar de fazer uma breve referência a três conceitos que estão presentes explicitamente ou mesmo implicitamente na LGPD e no RGPD e que requer a devida observância de seus destinatários e, portanto, repise-se, das Entidades Públicas (*in casu,* os TC's): a interoperabilidade (e sua relação com padrões de dados abertos); *privacy by design e privacy by default*; e *compliance* de dados.

É cediço que todo dado pessoal está registrado em um suporte, seja ele o papel, as unidades de memória, os serviços de hospedagem (com unidades de memória de grande capacidade de armazenamento); o sistema de computação em nuvem ou *cloud computing*, que representa um formato inovador na transferência, armazenamento e compartilhamento de dados, além de permitir a gestão de informações sob o controle do usuário, na medida em que estimula o armazenamento descentralizado em vários dispositivos, bem como viabiliza o acesso em qualquer lugar, formatação e em larga escala. A par disso, as legislações de proteção de dados preconizam que as Entidades Públicas deverão manter os dados em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de

[112] Cfe. FAZENDEIRO, Ana. *Regulamento geral sobre proteção de dados*. Coimbra: Almedina. 2018. p. 53.

[113] MELO, Antônio. *Estudo sobre a avaliação de impacto sobre a proteção de dados*. Disponível em: <www.tcontas.pt/geral>. Acessado em: 22 de fev. de 2020.

políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral (Art. 25 da LGPD).

Para que seja alcançado o formato interoperável e estruturado acima mencionado, é preciso envidar esforços para desenvolver programas de computador (*software*[114]) que corresponda a padrões abertos de tecnologia, em contraposição aos chamados padrões tecnológicos fechados, ou *software* proprietário, que são os programas de computador cujo autor não permite aos usuários ou terceiro o acesso ao seu código de programação, impedindo qualquer interação que não seja a utilização corriqueira. Um programa somente corresponde de fato a padrões abertos, quando preserva quatro tipos de liberdade dos seus usuários, quais sejam: execução, estudo, redistribuição de cópias e liberdade para modificação.

Além disso, os dados abertos também são pautados por três leis. As três leis dos dados abertos não são leis no sentido literal e, sim, um conjunto de testes para avaliar se um dado pode, de fato, ser considerado aberto. Elas foram propostas pelo especialista em políticas públicas, ativista dos dados abertos e palestrante de políticas públicas na Harvard Kennedy School of Government, David Eaves[115]. São elas: i) se o dado não pode ser encontrado e indexado na Web, ele não existe; ii) se não estiver aberto e disponível em formato compreensível por máquina, ele não pode ser reaproveitado; e iii) se algum dispositivo legal não permitir sua replicação, ele não é útil. Tais leis foram propostas para os dados abertos governamentais, mas pode-se dizer que elas se aplicam aos dados abertos de forma geral, mesmo fora de ambientes governamentais. Por exemplo, em empresas privadas, organizações da sociedade civil e organismos internacionais. O Banco Mundial, por exemplo, disponibiliza dados abertos. Nos últimos anos, especialistas têm discutido a abertura de dados pelo setor privado para ações que beneficiam o interesse público, os chamados "colaborativos de dados"[116].

Uma publicação intitulada "5 motivos para a abertura de dados na Administração Pública", elaborada pelo Tribunal de Contas da União - TCU, apresenta razões para que as organizações públicas invistam em iniciativas de abertura de dados governamentais. Os cinco motivos para a abertura dos

---

[114] A Lei n° 9.609/1998, de 19 de fevereiro de 1998, em seu Art. 1° assim define Software: é a expressão de um conunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em màquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de odo e para fins determinados. Disponível em: <www. http://legis.senado.leg.br/norma>. Acessado em: 20 de jan. de 2020.

[115] A public policy entrepreneur, open government activist and negotiation expert, David is a Lecturer of Public Policy at the Harvard Kennedy School of Government. At HKS, he teaches on digital transformation, service delivery, open government and open data. Disponível em: <https://eaves.ca/about-david>. Acessado em: 20 de jan. de 2020.

[116] Portal brasileiro de dados abertos. "*O que são dados abertos*?". Disponível em: <http://www.dados.gov.br/pagina/dados-abertos>. Acessado em: 20 de jan. de 2020.

dados são: transparência na gestão pública; contribuição da sociedade com serviços inovadores ao cidadão; aprimoramento na qualidade dos dados governamentais; viabilização de novos negócios; e obrigatoriedade por lei[117].

A LAI do Brasil (Lei n° 12.527/2011) e a Lei que aprova o regime de acesso à informação administrativa e ambiental e de reutilização dos documentos administrativos de Portugal (Lei n° 26/2016, de 22 de agosto de 2016) cuja aplicação é de observância obrigatória dos órgãos públicos e Entidades da Administração Pública prescrevem o formato aberto dos dados com vistas a tornar efetivo os Princípios da Transparência, da Publicidade, da igualdade, da proporcionalidade, da justiça, da imparcialidade e da colaboração com os particulares.

Nos termos da alínea "c" do n°.1 do Art. 3° da Lei n° 26/2016, "formato aberto" é um formato de ficheiro disponibilizado ao público e reutilizável independentemente da plataforma utilizada, nos termos do regime jurídico que regula a adoção de normas abertas para a informação em suporte digital na Administração Pública; ao passo que, ao dispor sobre transparência ativa, a LAI traz consigo conceitos de dados abertos, em especial em seu art. 8º, ao dispor que é dever dos órgãos e entidades públicas promover, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas.

Além disso, as legislações impõem aos órgãos e entidades públicas o dever de utilizar todos os meios e instrumentos legítimos de que dispuserem, sendo obrigatória a divulgação em sítios oficiais da rede mundial de computadores (internet) que, entre outros requisitos, deve possibilitar a gravação de relatórios em diversos formatos eletrônicos, inclusive abertos e não proprietários, tais como planilhas e texto, de modo a facilitar a análise das informações e possibilitar o acesso automatizado por sistemas externos em formatos abertos, estruturados e legíveis por máquina. Contudo, é de bom alvitre deixar registrado que devem ser consideradas as hipóteses de sigilo e de informações pessoais a serem observadas e que são exceções à regra geral de que os dados devem ser abertos.

Os conceitos a seguir analisados, quais sejam, o de privacidade desde a concepção e de privacidade por padrão (privacy by design e by default, respectivamente), têm a ver com as boas práticas em segurança da informação. Assim considerando, os agentes de tratamento ou qualquer outra pessoa

[117] "Cinco motivos para abertura de dados na Administração Pública". Disponível em: <https://portal.tcu.gov.br/biblioteca-digital/cinco-motivos-para-a-abertura-de-dados-na-administracao-publica.htm>. Acessado em: 20 de jan. de 2020.

.

que participe das fases do "ciclo de vida"[118] do tratamento de dados pessoais são obrigados a assegurar a segurança da informação para proteção dos dados pessoais, pois ambas estão relacionadas, além de que o dado pessoal é coletado para atender a uma finalidade específica e pode, por exemplo, ser eliminado a pedido do titular dos dados (conforme inciso IV, do Art. 18 da LGPD), ao cumprimento de uma sanção aplicada pela ANPD (conforme inciso VI, do Art. 52, da LGPD) ou ao término de seu tratamento (conforme Art. 16, da LGPD).

Com efeito, a proteção dos dados pessoais é alcançada por meio de medidas de segurança, técnicas e administrativas adotadas pelos agentes de tratamento, as quais visam proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, a teor do Art. 46 da LGPD. O Art. 32° do RGPD impõe aos responsáveis pelo tratamento de dados e subcontratante o dever de implementar medidas técnicas e organizativas adequadas, tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades sdas pessoas singulares.

Ocorre que tais medidas deverão ser observadas desde a fase de concepção do produto ou do serviço, durante todo o ciclo de vida do projeto, sistema ou processo, até a sua execução (§2°, do Art. 46 da LGPD) o que, em outras palavras, leva-nos a um conceito fundamental para a proteção da privacidade dos dados pessoais denominado "Privacidade desde a Concepção" ou *Privacy by Design*[119]. Por outro lado, a "Privacidade por padrão", ou *"Privacy by default"*[120], contempla uma perspectiva mais operacional, vinculada à definição de funcionalidades que por essência preconizam a proteção de dados pessoais, de que são exemplos a minimização, a exclusão, a anonimização e a pseudonominização de dados.

Na LGPD, a Privacidade por Padrão está diretamente relacionada ao princípio da necessidade, expresso pelo inciso III, do art. 6º, ao prever que as atividades de tratamento de dados pessoais deverão observar a boa-fé e alguns princípios, entre eles o da necessidade (inciso III), assim proclamado: '*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*'. A seu turno, a Privacidade desde a Concepção é alcançada por meio da aplicação de 7 (sete)

---

[118] Para orientar a prática do tratamento e apresentar os ativos institucionais envolvidos, divide-se o ciclo de vida do tratamento dos dados pessoais em cinco fases: coleta, retenção, processamento, compartilhamento e eliminação. Disponível em:, <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia>. Capítulo 3, p. 41. Acessado em: 26 de abr. de 2020.

[119] "*What does data protection 'by design'and 'bt default' mean"?* European Commission. Disponível em: <https://e.europa.eu/info/law-topc/data-protection/reform/rules-business-and-organisations/>. Acessado em: 20 de jan. de 2020.

[120] Ibid.

princípios fundamentais estudados por Cavoukian[121], quais sejam: medidas proativas e não reativas; privacidade adotada como padrão dos sistemas de tecnologia da informação; privacidade incorporada ao projeto (*design*); funcionalidade total (satisfação de todos os objetivos do projeto); segurança e proteção de ponta a ponta durante o ciclo de vida de tratamento dos dados; preservação da visibilidade e Transparência; e respeito à privacidade do utilizador.

Para finalizar este tópico de conceitos gerais, é interessante compreender a relevância que os programas de *compliance* assumem na tutela da proteção dos dados pessoais e no direcionamento dos agentes de tratamento a respeito das condutas necessárias para estarem em conformidade com os preceitos legais do RGPD e LGPD.

Compliance refere-se ao conjunto de ações a serem adotadas no ambiente corporativo para que se reforce anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade[122]. Trata-se da estruturação de políticas e procedimentos corporativos que se traduzam em ações sistemáticas com o objetivo de atender ao cumprimento aos preceitos normativos[123], a permitir a prevenção do ato ilícito ou, caso tal não seja possível, minorar seus efeitos e sancionar eventuais responsáveis. É, portanto, um conjunto de medidas, ferramentas e disciplinas adotadas pelas empresas, organizações, Entidades Públicas, para se fazer cumprir as normas legais e regulamentares. Neste sentido, tem sido as iniciativas do TC. de Portugal e, igualmente, mas ainda incipientes, os estudos realizados pelos TC's do Brasil.

Os programas de conformidade (*compliance programs*) são sistemas formais de políticas e procedimentos adotados por empresas e outras organizações projetadas para detectar e impedir violações da lei por funcionários e outros agentes e promover culturas éticas nos negócios[124]. Estes programas têm assumido relevância ante a ampliação do papel sancionador e regulador do Estado, cujas determinações legais servem de paradigma na construção de políticas de compliance, na medida em que procura fixar por meio de previsão legal, ou mesmo valorando os programas de compliance na aplicação de sanções,

---

[121] Cavoukian, Ann. Privacy by Design: The 7 Foundational Principles. August, 2009. Disponível em: <https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%20>. Acessado em: 13 jan. 2020.

[122] FRAZÃO, Ana. Programas de compliance e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. In: ROSSETTI, Maristela Abla; PITTA, Andre Grunspun. Governança corporativa: avanços e retrocessos. São Paulo: Quartier Latin, 2007. p. 42.

[123] Os programas de compliance, também chamados de programas de conformidade, de cumprimento ou de integridade, são instrumentos de governança corporativa tendentes a garantir que as políticas públicas sejam implantadas com maior eficiência" (CUEVA, Ricardo Villas Bôas. Funções e finalidades dos programas de compliance. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. Compliance: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018. p. 53)

[124] "Compliance programs are formal systems of policies and procedures adopted by corporations and other organizations that are designed to detect and prevent violations of law by employees and other agents and to promote ethical business cultures" (BASRI, Carole Basri. Corporate compliance. Carolina Academic Press. Edição do Kindle, 2017. p. 4.

fórmulas e conteúdos mínimos a serem observados pelas normas das empresas e Entidades Públicas.

No âmbito das entidades corporativas e, em alguns aspectos, também da Administração Pública e, repise-se, dos Tribunais de Contas, para que um programa de *compliance* seja efetivo há que se considerar na sua elaboração, no mínimo, dez requisitos[125]: proceder a uma avaliação contínua de riscos e atualização do programa; elaboração de Códigos de Ética e Conduta; organização compatível com o risco da atividade; comprometimento da alta administração; autonomia e independência do setor de *compliance*; realização de treinamentos periódicos; criar uma cultura corporativa de respeito à ética e às leis; monitoramento constante dos controles e processos, inclusive para fins de atualização do programa; canais seguros e abertos de comunicação de infrações e mecanismos de proteção dos informantes; e detecção, apuração e punição de condutas contrárias ao programa de compliance.

O compliance de dados pessoais presta-se justamente a auxiliar os agentes de tratamento na aplicação de forma eficaz das normas de proteção de dados, o que levará às empresas, Entidades Públicas e demais pessoas jurídicas a manter os dados e toda sua atividade dentro dos ditames legais, utilizando a segurança da informação em prol da minimização de incidentes que possam redundar em responsabilidade e consequente sanções.

Sob essa perspectiva, percebe-se facilmente que, às vantagens tradicionalmente atribuídas aos programas de compliance – (i) permitir a adequada gestão do risco da atividade – na medida em que identifica os pontos sensíveis em que há exposição ao descumprimento – e, por consequência, auxiliar na prevenção de ilícitos; (ii) viabilizar a pronta identificação de eventual descumprimento, bem como a remediação de danos daí decorrentes, auxiliando, assim, na minoração dos prejuízos; (iii) fomentar a criação de uma cultura corporativa de observância às normas legais; e (iv) servir potencialmente como atenuante no caso de punições administrativas[126] –, na tutela de dados, soma-se a vantagem adicional de adaptar e operacionalizar diversos dos comandos gerais e conceitos abertos da LGPD e do RGPD.

Verifica-se, pois, que o primeiro requisito a ser observado na construção de um programa de compliance de proteção de dados efetivo é a identificação dos riscos relacionados à atividade do agente de tratamento, o que torna necessário possuir o conhecimento do fluxo de dados existente na organização. Por isto, é de suma importância o mapeamento de todo o ciclo de dados e de suas principais

---

[125] FRAZÃO, Ana; MEDEIROS, Ana Rafaela Martinez., Desafios para a efetividade dos programas de compliance. In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. Compliance: perspectivas e desafios dos programas de conformidade. Belo Horizonte. 2018. p. 90-104.

[126] "*In essence, an effective compliance program can help insulate a company, and its officers, directors and employees from criminal and civil penalties; protect its officers and directors from personal liability; and create a culture of a 'good citizen' corporation. In fact, an effective compliance program can be a mitigating factor even if it failed to prevent a criminal offense*" (BASRI, Carole Basri. Corporate compliance. Carolina Academic Press. Edição do Kindle, 2017. p. 8-9).

características,[127] posto que vários são os fatores que podem influenciar no nível de risco, em especial a característica dos dados tratados; a destinação que lhes é conferida; e a forma como são coletados, utilizados e armazenados. Neste sentido, o Relatório de Impacto à Proteção de Dados Pessoais funciona como valiosa ferramenta de *compliance*, na medida em que possui como conteúdo mínimo exatamente tais elementos,[128] sendo recomendável que se efetue tal procedimento.

CAPÍTULO II – Enquadramento legal

2.1. O Âmbito de Aplicação Material do Regulamento Geral sobre Proteção de Dados (UE) 2016/679

O âmbito de aplicação material de um diploma normativo no dizer jurídico e em sentido amplo refere-se às matérias sobre as quais incidem as disposições legais e, em se tratando de legislação específica, a exemplo do RGPD (UE) 2016/679, a abrangência limita-se ao escopo para o qual a lei foi criada. Uma breve abordagem sobre o conteúdo material do retrocitado Regulamento faz-se necessária, eis que serviu de base para elaboração de legislações de diversos países, a exemplo da LGPD do Brasil.

O RGPD, que revogou e substituiu as regras então vigentes de proteção de dados, as quais possuíam mais de 20 anos de existência – Diretiva 95/46/CE, foi construído com o objetivo precípuo de eliminar as assimetrias existentes nos diferentes regimes de proteção de dados em vigor nos diferentes países da União Europeia, as quais constituiam um visível empecilho ao funcionamento do Mercado Único. A sua edição representou, em sua essência, uma mudança de paradigma no modelo de tratamento de dados pessoais e da livre circulação destes dados, posto que outros diplomas já tratara, em seu bojo, da matéria "proteção de dados", *e.g.* do art. 8° da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais[129].

---

[127] Cfe. FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. In: Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro: "*Aludido procedimento foi expressamente indicado na Comunicação da Comissão ao Parlamento Europeu e ao Conselho, concernente a Orientações relativas à aplicação do Regulamento Geral sobre a Proteção de Dados a partir de 25 de maio de 2018: é importante que os responsáveis pelo tratamento e os subcontratantes realizem revisões rigorosas aos respectivos ciclos da política de dados, por forma a identificarem claramente quais os dados que conservam, para que fins e que base jurídica (por exemplo, ambiente nuvem; operadores do setor financeiro)*" p. 6, Disponível em: <https://eur-lex.europa.eu/legal>. Acessado em 22 de dez. de 2019.

[128] "O relatório de impacto é a documentação que contém todo o ciclo de vida dos dados tratados, os procedimentos e riscos envolvidos, e as medidas que visam mitigar os riscos e/ou remediar os incidentes". Cfe: SANTOS, Fabiola Meira de Almeida; TALIBA, Rita. Lei Geral de Proteção de Dados no Brasil e os possíveis impactos. Revista dos Tribunais On-line, São Paulo, 2018. v. 998, p. 4.

[129] Artigo 8°

Direito ao respeito pela vida privada e familiar

Ante a necessidade de uniformizar o regime de proteção de dados pessoais nos países que integram o Espaço Europeu, o RGPD, diferentemente da Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, apresenta um conjunto de direitos dos titulares de dados pessoais e de obrigações de tratamento de dados que se impõem aos Responsáveis pelo Tratamento e Subcontratantes. Vale dizer, o Regulamento goza de aplicação direta na ordem jurídica de cada Estado Membro, não carecendo de transposição para o ordenamento jurídico interno, o que garante um tratamento uniforme de seu conteúdo em todos os Estados da União Europeia e, fora deles, quando estiver envolvido o tratamento de dados de cidadão europeu.

A par do esboçado âmbito territorial do art. 3°[130], o RGPD estabelece um conjunto de regras e obrigações tanto às organizações privadas quanto às públicas, cujas gestões deverão necessariamente ter em conta as matérias de Proteção de Dados. Ademais, inovou em direitos dos titulares de dados, e na previsão de cominação de coimas elevadíssimas pelo descumprimento de seus preceitos.

É importante destacar que o Regulamento, conquanto não pareça tão extenso, eis que conta com apenas 99 artigos, para ser assimilado em seu conteúdo requer seja feita uma leitura atenta dos 173 (cento e setenta e três) considerandos, essenciais a sua intepretação e completo entendimento. Naturalmente, não é objetivo deste trabalho enveredar por este caminho, senão abordar sucintamente o conteúdo que guarda relação com o tema que ora se desenvolve.

---

1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.

2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem - estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros. O acesso à legislação europeia pode dar-se por diversos sítios eletrônicos. Disponível em: <https://eur-lex.europa.eu/summary/glossary/eu_human_rights_convention.html?locale=pt>. Acessado em: 14 de jan. de 2020.

[130] Artigo 3.º

Âmbito de aplicação territorial

1. O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União.

2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares que se encontrem no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com:

a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento;

b) O controlo do seu comportamento, desde que esse comportamento tenha lugar na União.

3. O presente regulamento aplica-se ao tratamento de dados pessoais por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público. Cfe. FAZENDEIRO, Ana. Regulamento Geral sobre Proteção de Dados. 3 ed. – (textos da lei). Coimbra. ALMEDINA. 2018. p. 134.

Já no item 1 do art. 1°, o Regulamento, ao delinear o objeto e objetivos, deixa claro o âmbito de aplicação material a que se presta, o qual é reforçado no art. 2°, declarando com exatidão o conteúdo a ser observado ao serem aplicadas as suas regras.[131]

Os considerandos (1) e (2) do RGPD afastam quaisquer tipos de questionamentos relativos ao tratamento a ser dado aos dados pessoais, posto que elevam a proteção das pessoas singulares ao nível de direito fundamental, impondo respeito a esta matéria aos princípios e regras a serem aplicados, independentemente da nacionalidade ou do local de residência dessas pessoas e, para isso, invocam o Art. 8°, n° 1, da CDFUE[132], e o Art. 16°, n° 1, do TFUE[133].

No que concerne ao tratamento informático dos dados devem ser observadas duas características essenciais de segurança, a saber: a segurança no acesso à aplicação ou sistema pela utilização de password ou outro método de autenticação; e a possibilidade de rastreamento dos acessos. Contudo, na ótica do RGPD, a aplicação tem um alcance ainda maior, posto que visa garantir os direitos do titular dos dados e os princípios aplicáveis ao tratamento de dados pessoais.

Com efeito, o Art. 5° do capítulo II do RGPD enumera alguns princípios a serem considerados

---

[131] Artigo 1°.

Objeto e objetivos

1. O presente regulamento estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Artigo 2°.

Âmbito de aplicação material

1. O presente regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados.

2. O presente regulamento não se aplica ao tratamento de dados pessoais:

a) Efetuado no exercício de atividades não sujeitas à aplicação do direito da União;

b) Efetuado pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação do título V, capítulo 2, do TUE;

c) Efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas;

d) Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública..

3. O Regulamento (CE) n° 45/2001 aplica-se ao tratamento de dados pessoais pelas instituições, órgãos, organismos ou agências da União. O Regulamento (CE) n° 45/2001, bem como outros atos jurídicos da União aplicáveis ao tratamento de dados pessoais, são adaptados aos princípios e regras do presente regulamento nos termos previstos no artigo 98°.

4. O presente regulamento não prejudica a aplicação da Diretiva 2000/31/CE, nomeadamente as normas em matéria de responsabilidade dos prestadores intermediários de serviços previstas nos seus artigos 12° a 15°. Disponível em: Cfe. FAZENDEIRO, Ana. Regulamento Geral sobre Proteção de Dados. 3 ed. – (textos da lei). Coimbra. ALMEDINA. 2018. p. 133-134.

[132] Artigo 8°

Proteção de dados pessoais

1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. Cfe: SILVEIRA, Alessandra. *Tratado de Lisboa*.Versão Consolidada. 4. Ed. Lisboa: Quid Juris. 2019, p.363.

[133] Artigo 16°

(ex-artigo 286 - TCE)

1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. Ibid. p.77.

no tratamento de dados pessoais, cujo cumprimento é de observância obrigatória pelo responsável pelo tratamento, o qual detém ainda o poder de comprovação (princípio da responsabilidade).

Assim, pelo princípio da licitude, lealdade e transparência, somente podem ser objeto de tratamento os dados nos quais estejam presentes algum dos fundamentos de tratamento constantes do Art. 6.º (licitude do tratamento), devendo o tratamento encontrar-.se devidamente enquadrado no que foi efetivamente transmitido ao titular no momento da recolha e com a possibilidade de haver a verificação de como é feito o tratamento por parte do titular dos dados.

Pelo princípio da limitação das finalidades, devem os dados ser recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de uma forma incompatível com tais finalidades ou distintas delas, exceto no caso da existência de interesse superior que assim determine, como, por exemplo, para fins de arquivo de interesse público). Além disso, o princípio da conservação impõe um limite, qual seja, o de que os dados devam ser conservados somente durante o tempo estritamente necessário para as finalidades para as quais forem tratados.

O princípio da minimização dos dados evita o excesso, posto que, por sua observância, os dados pessoais recolhidos devem ser adequados, pertinentes e limitados ao que é necessário, devendo, contudo, serem exatos e atualizados sempre que necessário, conforme o princípio da exatidão.

Na ótica do princípio da integridade e confidencialidade, deverão os dados receber um tratamento que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental.

Isto posto, convém reportar-nos aos considerandos (15) e (16) do RGPD, os quais fazem referência expressa ao disposto no supra evidenciado artigo 2° e que são *per si* auto explicativos, senão vejamos. O primeiro deles, dispõe que "*a fim de se evitar o sério risco de ser contornada a proteção das pessoas singulares, esta deverá ser neutra em termos tecnológicos e deverá ser independente das técnicas utilizadas. A proteção das pessoas singulares deverá aplicar-se ao tratamento de dados pessoais por meios automatizados, bem como ao tratamento manual, se os dados pessoais estiverem contidos ou se forem destinados a um sistema de ficheiros. Os ficheiros ou os conjuntos de ficheiros bem como as suas capas, que não estejam estruturados de acordo com critérios específicos, não deverão ser abrangidos pelo âmbito de aplicação do presente regulamento*". Por sua vez o segundo assevera que [...] *"o regulamento não se aplica às questões de defesa dos direitos e das liberdades fundamentais ou da livre circulação de dados pessoais relacionados com atividades que se encontrem fora do âmbito de aplicação do direito da União, como as que se prendem com a segurança nacional. O presente regulamento não se aplica ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades realcionadas coma pol;itica externa e de segurança comum da União".*

Notadamente, em relação ao considerando (16), vemos a preocupação do legislador com as questões referidas também na alínea "b", do inciso 2 do art. 2°, o qual faz referência ao capítulo 2, do Título V do TUE e que trata tão somente das políticas relativas aos controlos nas fronteiras, ao asilo e à imigração. Vale dizer, estas questões foram afastadas do âmbito de aplicação material, por envolverem assuntos relativos à preservação da soberania dos Estados-Membros.

Para fechar este tópico, urge tecer breves linhas acerca dos direitos dos tirulares desses dados, eis que a Constituição Portuguesa e o próprio Regulamento resguardam-no em toda sua extensão. Tanto é assim que, a razão pela qual foi criado o RGPD, qual seja, uniformizar o regime de tratamento de dados no espaço da UE, considerou o respeito aos direitos dos titulares de dados um requisito essencial para o bom funcionamento do Mercado Único.

Destarte, o RGPD dedicou o Capítulo III aos direitos do titular dos dados, os quais estão detalhados em cinco secções, que vão do artigo 12° ao artigo 23°, sendo a última secção a que trata das limitações do alcance das obrigações e desses direitos. O titular dos dados tem os seguintes direitos: a ser informado; de acesso a seus dados; à retificação de seus dados; a ser esquecido ou apagado; à restrição de processamento; à portabilidade de dados; de oposição; a decisões individuais automatizadas, incluindo a definição de perfis.

O exercício dos direitos do titular passa pela ação do EDP, ou *Data Protection Officer* (DPO), figura esta que não existia na Diretiva 95/46/CE, embora já prevista na legislação de diversos países da Europa, a exemplo da lei alemã, a qual serviu de inspiração para o RGPD. Convém destacar que o Art. 37° do Regulamento obriga a designação do encarregado de proteção de dados para as autoridades e organismos públicos, o que é aplicável aos Tribunais de Contas; para as entidades que procedam a tratamentos em larga escala de dados pessoais sensíveis; e para as entidades que procedam também a tratamentos em larga escala de dados pessoais, desde que exijam um controlo regular e sistemático dos titulares dos dados. Em relação aos direitos dos titulares de dados, o n° 4 do Art. 38° dispõe que *"os titulares dos dados podem contactar o encarregado da proteção de dados sobre todas questões relacionadas com o tratamento dos seus dados pessoais e com o exercício dos direitos que lhe são conferidos pelo presente regulamento"*.

Por fim, registre-se que a implementação das regras previstas no RGPD, no que atine ao âmbito de aplicação material, notadamente em relação à garantia dos direitos dos titulares dos dados a serem tratados, implica para as entidades privadas e públicas a adoção de soluções técnicas que lhes permitam dar respostas adequadas e satisfatórias às solicitações formulads pelos titulares dos dados, sob pena de descumprimento de suas normas e consequente cominação das penalidades previstas.

2.2 Tratamento de dados pessoais pelos órgãos ou agências da União Europeia

Em relação ao tratamento de dados pessoais por instituições, órgãos comunitários, organismos ou agências da União, o n° 3 do Art. 2° do RGPD remete o tratamento de dados pessoais ao Regulamento (CE) n° 45/2001, de 18 de dezembro de 2000, do Parlamento Europeu e do Conselho[134], contudo estabelece expressamente a necessidade de que os dispositivos que neste último regulam a matéria e outros actos jurídicos da União sejam adaptados aos seus princípios e regras. Ocorre, entretanto, que o Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018[135], relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados revogou o Regulamento (CE) n.º 45/2001 do Parlamento Europeu e a Decisão n.º 1247/2002/CE[136]. Portanto, para efeitos de aplicação ao tratamento de dados pessoais por instituições, órgãos comunitários, organismos ou agências da União, a referência será feita ao Regulamento (UE) 2018/1725.

Uma primeira observação importrante a ser feita, refere-se ao que dispõe o considerando (5) do Regulamento (UE) 2018/1725, posto que afasta quaisquer dúvidas e ambiguidades que pudessem vir a surgir na aplicação simultânea daquele regulamento e do RGPD. Com efeito, assim explicita o retrocitado considerando: "*uma abordagem coerente da proteção dos dados pessoais e a livre circulação dos mesmos na União implicam uma harmonização, tão ampla quanto possível, das regras de proteção de dados adotadas a nível das instituições, dos órgãos e dos organismos da União com as regras de proteção de dados adotadas para o sector público nos Estados-Membros. Sempre que as disposições do presente regulamento sigam os mesmos princípios que as disposições do regulamento (UE) 2016/679, de acordo com a jurisprudência do Tribunal de Justiça da União Europeia («Tribunal de Justiça»), esses dois conjuntos de disposições deverão ser interpretados de forma homogénea, sobretudo porque o regime do presente regulamento deverá ser entendido como equivalente ao regime do Regulamento (UE) 2016/679*".

---

[134] Regulamento (CE) n.° 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados. (Jornal Oficial das Comunidades Européias - L 8 de 12.1.2001, p. 1). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=OJ%3AL%3A2001%3A008%3ATOC> . Acessado em: 02 de fev. 2020.

[135] Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=CELEX:32018R1725>

[136] Decisão do Parlamento Europeu, do Conselho e da Comissão, de 1 de julho de 2002, relativa ao estatuto e às condições gerais de exercício de funções da autoridade europeia para a protecção de dados. Disponível em: <https://eur-lex.europa.eu/search.html?qid=1594410130030&text=Decis%C3%A3o%20n.%C2%BA%201247/2002/CE&scope=EURLEX&type=quick&lang=pt>. Acessado em: 02 de fev. 2020.

O Art. 2° do Regulamento delimita o âmbito de aplicação de suas regras, as quais abarca todas as instituições, órgãos e organismos da União, no tocante ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios distintos dos meios automatizados de dados pessoais contidos em ficheiros ou a eles destinados. Exclui, entretanto, os ficheiros ou os conjuntos de ficheiros, bem como as suas capas, que não estejam estruturados de acordo com critérios específicos.

Ainda com relação ao âmbito de aplicação, há de se fazer duas distinções: as regras gerais relativas ao tratamento de dados pessoais operacionais e as regras específicas aplicáveis ao tratamento de dados pessoais operacionais pelos órgãos e organismos da União no exercício de atividades abrangidas pelo âmbito de aplicação da Parte III, título V, capítulos 4 ou 5, do TFUE[137].

É importante ressaltar que as regras específicas tem natureza de *lex specialis,* relativamente ao tratamento de dados pessoais operacionais e, tendo em conta que *lex specialis derogat legi generali*[138], com o objetivo de diminuir a fragmentação jurídica, as disposições específicas hão de guardar coeréncia com os princípios subjacentes ao capítulo relativo ao tratamento de dados pessoais operacionais, e também com as disposições do presente regulamento relativas ao controlo independente, às vias de recurso, à responsabilidade e às sanções. Em síntese, é o que expõe o considerando (11).

No que diz respeito ao tratamento de dados pelas instituições, órgãos, organismos e agências da União e a livre circulação desses dados, e levando em conta a preocupação com a uniformização no tratamento e protecção de dados pessoais, é importante dedicar algumas linhas ao Capítulo IV do

[137] O Tratado sobre o Funcionamento da União Europeia (TFUE), na sequência do Tratado de Lisboa, foi desenvolvido a partir do Tratado que instituiu a Comunidade Europeia (TCE ou Tratado CE), conforme estabelecido pelo Tratado de Maastricht. O Tratado CE baseava-se, por sua vez, no Tratado que instituiu a Comunidade Económica Europeia (TCEE), assinado em Roma em 25 de março de 1957. A criação da União Europeia (UE) através do Tratado de Maastricht (7 de fevereiro de 1992) assinalou uma nova etapa no processo de unificação política da Europa. O TFUE é um dos dois tratados que constituem o direito primário da UE, juntamente com o Tratado da União Europeia (TUE). Constitui a base detalhada do direito da UE ao definir os princípios e objetivos da UE, bem como o âmbito de ação nos respetivos domínios de intervenção. Descreve também os detalhes organizacionais e funcionais das instituições da UE. Acerca destas regras, consultar a Parte III do TFUE, que trata das Políticas e Ações Internas da União e se desdobra no Título V (o Espaço de Liberdade, Segurança e Justiça), e em especial o Capítulo 4 (Cooperação Judiciária em Matéria Penal) e o Capítulo 5 (Cooperação Policial). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3A4301854> . Acessado em: 06 de fev. de 2020.

[138] Critério da Especialidade: também denominado *Lex specialis*, em função da expressão latina *lex specialis derogat legi generali*. Por esse critério, se as normas incompatíveis forem geral e especial, prevalece a segunda. O entendimento que norteia esse critério diz respeito à circunstância de a norma especial contemplar um processo natural de diferenciação das categorias, possibilitando, assim, a aplicação da lei especial aquele grupo que contempla as peculiaridades nela presentes, sem ferir a norma geral, ampla por demais. Além do mais, a aplicação da regra geral importaria no tratamento igual de pessoas que pertencem a categorias diferentes, e, portanto, numa injustiça. Disponível em: <https://jus.com.br/artigos/7207/das-antinomias-juridicas>. Acessado em: 06 de fev. de 2020.

Regulamento (UE) 2018/1725[139] do Parlamento Europeu e do Conselho, intitulado "Responsáveis pelo tratamento e subcontratantes", o qual disciplina as obrigações gerais (secção 1) dirigidas às pessoas envolvidas no tratamento dos dados; a segurança dos dados pessoais (secção 2); a confidencialidade das comunicações eletrónicas (secção 3); a avaliação de impacto relativa à protecção e consulta prévia (secção 4); informação e consulta legislativa (secção 5); e, por fim, o encarregado de protecção de dados (secção 6).

Tais secções estabelecem obrigações e requisitos aplicáveis quanto ao tratamento de dados pessoais, a saber: O n° 1 do Art. 26°, da secção 1, ao disciplinar sobre a responsabilidade dos responsáveis pelo tratamento, prescreve que estes tem a obrigação de aplicar medidas técnicas e organizativas adequadas que lhes assegurem e comprovem ser o tratamento realizado conforme as diretrizes do regulamento, bem como lhes dá a imcumbência de revisar e atualizar essas medidas sempre que for necessário. Também em relação à protecção dlos direitos dos titulares de dados desde a concepção (Art. 27°), o responsável pelo tratamento deve aplicar medidas técnicas e organizativas adequadas, destinadas a pôr efetivamente em prática os princípios da proteção de dados, a exemplo da pseudonimização, bem como estar seguro de que, por defeito, estas medidas sejam aplicadas apenas ao tratamento de dados pessoais necessários para cada finalidade específica do tratamento. Para efeitos de comprovação da conformidade das operações de tratamento de responsáveis pelo tratamento, os Estados-Membros, as autoridades de controlo, o Comité e a Comissão podem valer-se de procedimentos de certificação em matéria de proteção de dados, bem como selos e marcas de proteção de dados, nos termos do Art. 42° do RGPD.

Similarmente e em conformidade com o RGPD, o Regulamento (UE) 2018/1725, põe em relevo a proteção dos direitos e das liberdades dos titulares de dados. Tanto é assim que, ao tratar do tema responsabilidade dos envolvidos no tratamento de dados, leia-se responsáveis em sentido amplo (abrangendo subcontratantes, pessoas que não sejam instituições ou órgãos da União etc), exige uma clara repartição das responsabilidades, notadamente quando o responsável pelo tratamento determina as finalidades e os meios do tratamento conjuntamente com outros responsáveis, ou quando uma operação de tratamento é efetuada por conta de um responsável pelo tratamento. É o que se depreende da leitura do Art. 28° e, também do Art. 29° que, por seu turno, traz exigências específicas a serem observadas no

[139] Considerando (8): "O presente regulamento deverá aplicar-sr ao tratamento de dados pessoais por todas as instituições e por todos os órgãos e organismos da União. O presente Regulamento deverá aplicar-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios distintos dos meios automatizados de dados pessoais contidos em ficheiros ou a eles destinados. Os ficheiros ou os conjuntos de ficheiros, bem como as suas capas, que não estejam estruturados de acordo com critérios específicos, não deverão ser abrangidos pelo âmbito de aplicação do presente regulamento". Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1594414075505&uri=CELEX:32018R1725> . Acessado em: 06 de fev. de 2020.

tratamento por subcontratação, a exemplo da formalização dos serviços mediante a celebração de contrato ou outro ato normativo ao abrigo do direito da União ou do direito dos Estados-Membros, que vincule o subcontratante ao responsável pelo tratamento, que estabeleça o objeto e a duração do tratamento, a sua natureza e a sua finalidade, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e os direitos do responsável pelo tratamento, além da possibilidade de optar por um contrato individual ou por cláusulas contratuais-tipo adotadas diretamente pela Comissão, ou pela Autoridade Europeia para a Proteção de Dados e posteriormente pela Comissão.

A teor do Art. 30°, para que qualquer pessoa ou subcontratante agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, tenham acesso ao tratamento de dados pessoais, são exigidas instruções do responsável pelo tratamento, excepto se a tal for obrigado pelo direito da União ou pelo direito dos Estado-Membros. Vale ressaltar que as atividades de tratamento devem ser conservadas em registro próprio por cada responsável, conforme Art. 31°. De outra banda, ao ser concluído o tratamento por conta do responsável pelo tratamento, o subcontratante deverá devolver ou apagar os dados pessoais, consoante a escolha do responsável pelo tratamento, a não ser que a conservação desses dados pessoais seja exigida ao abrigo do direito da União ou do direito do Estado - Membro a que o subcontratante está sujeito[140].

A Secção 2[141] é dedicada à segurança dos dados pessoais e está didaticamente distribuída em três artigos, a saber: o art. 33°, que disciplina a segurança do tratamento; o Art. 34°, que traz regras referentes à Notificação de violações dos dados pessoais à Autoridade Europeia para a Proteção de Dados; e o art. 35° o qual refere-se à obrigação de comunicação de violações de dados pessoais ao titular dos dados, caso a violação seja suscetível de constituir um elevado risco para os direitos e as liberdades das pessoas singulares. O primeiro dos artigos supra mencionados estabelece que o responsável pelo tratamento e o subcontratante além de ter em conta os conhecimentos técnicos disponíveis, os custos de aplicação, e as finalidades do tratamento, entre outros aspectos, devem por em prática medidas técnicas e organizativas que garantam um nível de segurança adequado considerando os riscos do tratamento bem como a natureza dos dados pessoais objeto de proteção. O segundo impõe dois deveres de notificação em caso de violação de dados pessoais e uma obrigação de informação, a saber: ao responsável pelo tratamento o dever de notificação no prazo de 72 horas à Autoridade Europeia; ao subcontratante o dever de notificar o responsável, sem demora indevida; e ao responsável o de informar o encarregado de proteção de dados. Todas estas precauções objetivam sobretudo evitar o acesso ou divulgação não

[140] Cfe. Regulamento (UE) 2018/1725, cuja ementa foi devidamente explicitada em nota de referênccia acima. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1594414075505&uri=CELEX:32018R1725> . Acessado em: 06 de fev. de 2020.

[141] Ibid.

autorizados ou quaisquer danos ou anomalias na forma de tratamento.

As formalidades a serem observadas quanto à confidencialidade das comunicações eletrónicas, objeto da secção 3, do Capítulo IV, requerem a atuação das instituições e órgãos visando a garantia da segurança das respectivas redes de comunicações eletrónicas, posto que devem ser protegidas as informações transmitidas aos equipamentos terminais dos utilizadores que acedem aos seus sítios *web* e a aplicações móveis acessíveis ao público, conservada com eles relacionadas, e das informações tratadas e recolhidas através desses equipamentos, nos termos do n.° 3, Art. 5.°, da Diretiva 2002/58/CE[142]. Ademais, as instituições e os órgãos da União tem a obrigação de adotar as medidas necessárias com o objetivo de impedir que os dados pessoais inseridos em listas de utilizadores sejam utilizados para fins de *marketing* direto, ou seja, os acessos às listas devem limitar-se aos fins específicos das listas, consoante Art. 38°.

A secção 4 do Regulamento traz regras aplicáveis à proteção de dados em se tratando de um tipo de tratamento que venha a fazer uso de novas tecnologias, as quais possam vir a constituir um elevado risco para os direitos e as liberdades das pessoas singulares, caso em que a Autoridade Europeia para a Proteção de Dados deve estabelecer e tornar pública uma lista dos tipos de operações de tratamento sujeitos ao requisito de avaliação de impacto relativa à proteção de dados. Estas situações exigem uma ação diferenciada do responsável pelo tratamento, posto que este, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento, deve proceder, antes de iniciar o tratamento, a uma avaliação do impacto das operações de tratamento previstas na proteção de dados pessoais, a qual é precedida de um parecer do encarregado da proteção de dados.

Ainda em relação à avaliação de impacto, nos exatos termos do art. 40°, o responsável pelo tratamento deve consultar a Autoridade Europeia para a Proteção de Dados, antes de proceder ao tratamento, caso numa avaliação de impacto relativa à proteção de dados, haja a evidência de que o tratamento, na falta de garantias, de medidas e de procedimentos de segurança para atenuar os riscos, constitui um elevado risco para os direitos e as liberdades das pessoas singulares, e que o risco não poderá ser atenuado por meios razoáveis, tendo em conta as tecnologias disponíveis e os custos de aplicação. Também nestas situações, o encarregado da proteção de dados deverá emitir parecer sobre a

[142] Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas ("Diretiva relativa à privacidade e às comunicações eletrónicas")
Art. 5°.
3. Os Estados Membros asseguram que o armazenamento de informações ou a possibilidade de acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador só sejam permitidos se este tiver dado o seu consentimento prévio com base em informações claras e completas, nos termos da Directiva 95/46/CE, nomeadamente sobre os objectivos do processamento... Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32002L0058>. Acessado em: 14 de fev. 2020.

necessidade da consulta prévia. Em todo o procedimento, a Autoridade Europeia zelará pela observância do Regulamento e utilizará de seus poderes visando o fiel cumprimento das disposições nele contidas.

Similarmente ao que dispõe o RGPD, o Regulamento 2018/1725 (UE) estipula no Art. 25° algumas limitações à aplicação dos direitos dos titulares de dados insculpidos nos Arts. 14° a 22°, à comunicação de violações de dados pessoais ao titular dos dados (Art. 35°), à confidencialidade das comunicações eletrónicas (Art. 36°), bem como aos princípios relativos ao tratamento de dados pessoais (Art. 4°). Tais limitações, contudo, a teor do Art. 41° da secção 5, serão permitidas quando da elaboração de medidas administrativas e de regras internas relativas ao tratamento de dados pessoais por uma instituição ou por um órgão da União, sob a condiçào de que seja respeitada a essência dos direitos e das liberdades fundamentais dos titulares dos dados e desde que as instituições consultem e informem a Autoridade Europeia para a Proteção de Dados.

O Art. 43°, por sua vez, trata da figura do encarregado de proteção de dados, o qual será designado por cada instituição ou órgão da União, dentre seu pessoal, com conhecimentos especializados sobre a legislação e as práticas em matéria de proteção de dados, ou ainda que exerça suas funções com base num contrato de prestação de serviços. Os encarregados da proteção de dados deverão assegurar que as disposições do regulamento sejam aplicadas, e aconselhar os responsáveis pelo tratamento e os subcontratantes no cumprimento das suas obrigações e, para isso, necessário se faz desempenhar as suas funções e cumprir os seus deveres de forma independente.

Para finalizar este tópico, é de bom alvitre reportar-se a alguns organismos referidos tanto no Regulamento (UE) 2016/679 - RGPD quanto no Regulamento (UE) 2018/1725, os quais desempenham funções essenciais ao cumprimento desses diplomas. Neste desidério, o RGPD criou o Comité Europeu para a Proteção de Dados, como um organismo independente da União com personalidade jurídica, com o objetivo de contribuir para a aplicação escorreita do próprio RGPD e da Diretiva (UE) 2016/680 em toda a União, e como órgão de aconselhamento da Comissão. Pelo n° 1 do Art. 52° do Regulamento (UE) 2018/1725 "[...] é criada a Autoridade Europeia para a Proteção de Dados", a qual exerce com total independência as funções de supervisão, controlo e aplicação do Regulamento e de qualquer outro ato da União relativo à proteção dos direitos e liberdades fundamentais das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e órgãos da União, bem como a de aconselhamento das instituições e dos órgãos da União e dos titulares dos dados sobre todas as questões relativas ao tratamento de dados pessoais.

2.3 Regras Específicas do Poder Público no Brasil aplicáveis ao tratamento de dados pessoais

A nova LGPD tem sido vista e ocupado a sociedade brasileira principalmente sob uma perspectiva empresarial privada. Inobstante tal constatação, um de seus pontos mais relevantes diz respeito à aplicação das práticas de tratamento de dados no âmbito do setor público, em seus diversos poderes (Executivo, Legislativo e Judiciário) e entes federativos (União, Estados, Distrito Federal e Municípios), posto que estes se valem do tratamento de dados pessoais dos cidadãos, servidores, terceirizados etc, tanto para a elaboração e execução de políticas públicas, como também para o oferecimento de seus serviços à sociedade.

O tema proteção de dados pessoais objeto da LGPD, a qual apresenta, em seu Art. 6°, os princípios da boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas, não é novidade para o ordenamento jurídico do Brasil, posto que algumas legislações precedentes já abordavam à necessidade de se garantir a proteção de dados pessoais. A própria Constituição Federal de 1988, embora não discipline de forma específica a matéria, apresenta os fundamentos que objetivam a proteção de dados pessoais e, no Título II, dos “”Direitos e Garantias Fundamentais”, elenca expressamente os direitos à intimidade, à vida, à privacidade, à igualdade, à liberdade e ao acesso à informação, além de tratar importantes garantias em Institutos Jurídicos, que em muito se assemelha à concepção atual referente à guarda de informações, a exemplo do *“Habeas data”*[143].

Isto posto, é imprescindível compreender qual o impacto que a LGPD provocará em cada ente que compõe a Administração Pública no Brasil e, para isso, é mister buscar às definições que o Direito Administrativo traz referente aos órgãos e entidades constituintes do Poder Público, no tocante à natureza jurídica do ente e em qual interesse age - se no interesse público e em sua finalidade ou em regime concorrencial. Vale lembrar que *“[...] o ordenamento jurídico brasileiro submete as variadas hipóteses de atuação da administração pública, nos três poderes e em todos os níveis da Federação, ora a um regime jurídico tipicamente de direito público, ora a normas oriundas predominantemente do*

[143] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

LXXII - conceder-se-á habeas data:

a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;

direito privado"[144], conforme assevera Marcelo Alexandrino e Vicente Paulo ao referir-se sobre o regime jurídico-administrativo.

Levando em conta o que se expôs acima, verifica-se que o uso da tecnologia da informação e das técnicas de tratamento de dados tem sido cada vez mais explorado pela administração pública como importante instrumento para a gestão pública, a exemplo dos programas de Governo Eletrônico[145] (*eGOV*) e das experiências com as conhecidas "cidades inteligentes"[146], os quais, *per si,* enseja uma atenção especial para o tratamento de dados pessoais na perspectiva do setor público. A par disso, a LGPD dedicou nove artigos em seu capítulo IV ao tratamento de dados pessoais pelo Poder Público, estabelecendo regras e responsabilidades ao tempo em que procurou harmonizar as disposições relativas ao acesso à informação nas mãos da administração pública com a proteção de dados pessoais dos cidadãos.

Neste item, procurar-se-á discorrer algumas linhas interpretativas sobre os dispositivos LGPD na perspectiva da aplicação pelo setor público, eis que há várias regras criadas pela lei especificamente para este fim, e.*g.* às relativas ao compartilhamento de dados pessoais, transparência e bases autorizativas dos tratamentos de dados pessoais exclusivas para órgãos e entidades públicas. Ademais, verifica-se a existência de algumas peculiaridades, a exemplo da previsão da aplicação de diferentes sanções a depender do regime concorrencial ou não da entidade pública, fato de relevante importância para empresas públicas e sociedades de economia mista, visto que atuam em regimes que se alternam entre a iniciativa privada e a gestão ou execução das políticas públicas.

Uma leitura atenta dos dispositivos da LGPD do Brasil, com as alterações promovidas pela Lei n° 13.853 de 2019, e notadamente nos limites do presente trabalho, permite-nos inferir que as pessoas jurídicas de direito público nas três esferas de governo (Federal, Estadual e Municipal)[147] as quais ela se aplica, vale dizer, que devam observar suas regras quando do tratamento de dados pessoais, abrange os

---

[144] Cfe. ALEXANDRINO, Marcelo; PAULO, Vicente. *Direito administrativo descomplicado*.- 24. Ed. Rio de Janeiro: Forense; São Paulo, 2107. P. 11

[145] Governo eletrônico, ou *e-gov*, consiste no uso das tecnologias da informação — além do conhecimento nos processos internos de governo — e na entrega dos produtos e serviços do Estado tanto aos cidadãos como à indústria e no uso de ferramentas eletrônicas e tecnologias da informação para aproximar governo e cidadãos. Disponível em: <https://www.infoescola.com/informatica/governo-eletronico/>, Acessado em: 12 de dez. de 2019.

[146] Uma Cidade Inteligente ou S*mart Cities* é uma área urbana que usa tipos diferentes de sensores eletrônicos da Internet das Coisas para coletar dados e usá-los para gerenciar recursos e ativos eficientemente. Disponível em: <https://fgvprojetos.fgv.br/noticias/o-que-e-uma-cidade-inteligente>, Acessado em: 12 de dez. de 2019.

[147] Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. Disponível em: <www.planalto.gov.br> . Acessado em: 12 de dez. de 2019.

órgãos públicos ou entidades públicas da administração direta bem como as empresas públicas e sociedades de economia mista, da administração indireta.

É o que se depreende da leitura do parágrafo único do art. 1º da lei 12.527/2011, a Lei de Acesso à Informação, relativamente ao tratamento de dados pessoais pelas pessoas jurídicas de direito público nele referidas, *in verbis*: I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público; II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios[148].

Contudo, o Art. 4° da LGPD excluiu de seu âmbito também para o Poder Público, os casos de tratamento de dados realizados para fins exclusivamente jornalísticos e artísticos; acadêmicos; bem como para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais. Excetua, ainda, os casos de tratamentos de dados provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado à LGPD.

Cabe salientar que, no caso de tratamentos de dados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou das atividades vinculadas a infrações, a LGPD estabelece algumas limitações ao tratamento de dados, embora não as enquadrem em seu âmbito de aplicação. É o que dispõe os §§ 1° ao 4°, da LGPD[149].

Em síntese, para aquelas finalidades exige-se legislação específica, que as medidas deverão deverão ser adequadas e devem atender ao interesse público e, quando o tratamento de dados para tais

---

[148] Disponível em: <www.planalto.gov.br> . Acessado em: 12 de dez. de 2019

[149] § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público,
observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.

§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à
proteção de dados pessoais.

§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo Poder Público. Disponível em: <www.planalto.gov.br> . Acessado em: 12 de dez. de 2019

finalidades for realizado por pessoa jurídica de direito privado, deverá estar sob a tutela de pessoa jurídica de direito público, excetuando-se as empresas controladas pelo Poder Público.

Destarte, e levando em conta a forte influência do RGPD sobre a LGPD, mormente em relação ao tratamento de dados pessoais pelo Poder Público, limitar-se-á o presente tópico a linhas interpretativas do Capítulo IV da legislação do Brasil, o qual se subdivide em duas sessões que vão do Art. 23° ao Art. 32°. A primeira das sessões diz respeito às regras a serem aplicadas, ao passo que a segunda dispõe sinteticamente acerca da responsabilidade.

Preliminarmente, cabe ressaltar a referência que o Art. 23 da LGPD faz ao Art. 1° da LAI que, como o próprio nome sugere, regula o acesso a informações previsto no inciso XXXIII do Art. 5º[150], no inciso II do § 3º do Art. 37[151] e no § 2º do Art. 216[152] da CRFB. Nos referidos artigos, a Constituição, de forma ampla e com base no princípio da igualdade, remete à lei ordinária a regulação do direito de acesso dos usuários a registros administrativos e a informações sobre atos de governo, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

De acordo com o prescrito na CRFB, a legislação infraconstitucional estabeleceu em seu Art. 23° que o tratamento de dados pessoais pelas pessoas jurídicas de direito público deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, com alguns requisitos especificados nos incisos I e III, a saber: I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; II - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais.

---

[150] Art. 5° Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado. Disponível em: <www.planalto.gov.br>. Acessado em 12 de jan. de 2019.

[151] Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte:
§ 3º A lei disciplinará as formas de participação do usuário na administração pública direta e indireta, regulando especialmente:
II - o acesso dos usuários a registros administrativos e a informações sobre atos de governo, observado o disposto no art. 5º, X e XXXIII; Disponível em: <www.planalto.gov.br>. Acessado em 12 de jan. de 2019.

[152] Art. 216. Constituem patrimônio cultural brasileiro os bens de natureza material e imaterial, tomados individualmente ou em conjunto, portadores de referência à identidade, à ação, à memória dos diferentes grupos formadores da sociedade brasileira, nos quais se incluem:
§ 2º Cabem à administração pública, na forma da lei, a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem. Disponível em: <www.planalto.gov.br>. Acessado em 12 de jan. de 2019.

Além destes requisitos, há de serem observados pelo Poder Público os prazos e procedimentos para exercício dos direitos do titular, para os quais deverão buscar o disposto em legislação específica, notadamente o constante na Lei nº 9.507, de 12 de novembro de 1997 (Lei do *Habeas Data*), na Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo), e também as disposições da Lei nº 12.527, de 18 de novembro de 2011 (LAI). Verifica-se uma preocupação do legislador em harmonizar o conteúdo das leis aplicáveis ao Poder Público de modo que não haja conflitos que venham a atropelar o exercício de direitos dos titulares, o que alcança não apenas seus servidores públicos como também pessoas singulares e demais jurisdicionados que tenham a obrigação legal de prestar informações às instituições e entidades públicas.

Uma importante distinção há de ser observada pelas empresas públicas e sociedades de economia mista, posto que se atuam em regime de concorrência, nos termos do Art. 173 da Constituição Federal[153,] aplica-se a elas o mesmo tratamento dispensado pela LGPD às pessoas jurídicas de direito privado, ao passo que se estiverem operacionalizando políticas públicas, o tratamento a ser dados será o mesmo aplicado aos órgãos e às entidades do Poder Público. Exemplo típico a ser dado é o caso da Caixa Econômica Federal, a qual é uma Empresa Pública de Direito Privado, um verdadeiro Banco Público, cujo capital é totalmente do Governo Federal. Esta instituição, ao atuar como um banco no manuseio dos dados de seus clientes, realizando empréstimos e operações similares, será norteada pelas regras da LGPD aplicáveis ao setor privado, ao passo que ao tratar dados pessoais no âmbito de programas governamentais sociais, e.g. o Seguro-Desemprego, tal Entidade passará a observar as regras da LGPD aplicáveis ao setor público. É o que se extrai do teor do Art. 24°.

Para a execução de políticas públicas, para a prestação de serviços públicos e com vistas à descentralização da atividade pública, à disseminação e ao acesso das informações pelo cidadão, os dados a serem coletados pelo Poder Público devem ser mantidos em formato interoperável e estruturado para o uso compartilhado (Art. 25°). Em se tratando do uso compartilhado de dados pessoais, a regra do artigo 26 é a de vedação ao compartilhamento dos dados em posse da Administração Pública com entidades privadas, exceto nos casos em que a transferência se faça necessária com o fim específico e determinado de execução descentralizada da atividade pública e, além disso, que sejam respeitados os princípios de proteção dos dados pessoais.

---

[153] **Art. 173.** Ressalvados os casos previstos nesta Constituição, a exploração direta de atividade econômica pelo Estado só será permitida quando necessária aos imperativos da segurança nacional ou a relevante interesse coletivo, conforme definidos em lei.**§ 1º** A empresa pública, a sociedade de economia mista e outras entidades que explorem atividade econômica sujeitam-se ao regime jurídico próprio das empresas privadas, inclusive quanto às obrigações trabalhistas e tributárias.**§ 1º** A lei estabelecerá o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias que explorem atividade econômica de produção ou comercialização de bens ou de prestação de serviços, dispondo sobre. Disponível em: <www.planalto.gov.br>. Acessado em 12 de jan. de 2020.

Acerca do tema descentralização, assim doutrina Maria Silvia Zanella de Pietro, "[...] a descentralização administrativa ocorre quando há distribuição de competências de uma para outra pessoa, física ou jurídica"[154], situação que se verifica quando o Estado atribui para uma empresa pública, uma autarquia, uma sociedade de economia mista, uma fundação pública, um consórcio público a execução de um serviço público ou mesmo nos casos das concessões, autorizações e permissões, onde um ente privado executa um serviço público em nome do Estado.

O Art. 27, a seu turno, determina que a comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá, em regra, de consentimento do titular, exceção feita aos casos de dispensa do consentimento; quando necessários para execução da atividade pública, em que será dada publicidade, nos termos do inciso I do caput do Art. 23; e nas exceções previstas no Art. 26 alhures comentadas.

A autoridade nacional tem atuação relevante determinada pela lei, no controle da atuação dos órgãos e às entidades do poder público quando da realização de operações de tratamento de dados pessoais, podendo solicitar informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado; emitir parecer técnico complementar para garantir o cumprimento da LGPD; estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais; solicitar a agentes públicos a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público; e, no tocante às infrações aos dispositivos da lei em decorrência do tratamento de dados pessoais por órgãos públicos, poderá enviar informe com medidas cabíveis para fazer cessar a violação.

Em relação aos órgãos do Setor Público, notadamente os que compõem a Administração Indireta, uma vez constatada a necessidade de tratamento de dados pessoais, em princípio deve o ente público identificar sob qual condição atua, posto que as consequências de atuar em regime concorrencial ou ao atendimento das finalidades públicas são distintas, não somente em relação aos requisitos exigidos como também a aplicação de sanções decorrentes do descumprimento ou da atuação em desconformidade com a lei. Eis que é neste aspecto, o dos requisitos a aplicar, onde se verifica a necessidade de atenção redobrada no tratamento dedicado às Entidades Públicas pela LGPD.

No tocante aos Tribunais de Contas do Brasil e, por conseguinte, ao TCE/RN e ao TCE/PB, em setembro de 2019, o Instituto Rui Barbosa[155] criou um Grupo de Estudos sobre a LGPD, de natureza

---

[154] DI PIETRO, Maria Sylvia Zanella. *Direito Administrativo* - 29.ed. Rev., atual. e ampl. - Rio de Janeiro: Forense, 2016. p.573.

[155] Cfe. Informação no Instituto Rui Barbosa – IRB, que é uma associação civil criadas pelos Tribunais de Contas do Brasil em 1973 com o objetivo de auxiliar os Tribunais no desenvolvimento e aperfeiçoamento das atividades dos Tribunais de Contas. É conhecido por ser o "braço acadêmico" do Sistema de Controle Externo, por conta dos seus eventos, seminários, congressos, revistas técnicas, livros, e

multidisciplinar, composto por membros do Comitê Técnico de Processo, Súmula e Jurisprudência (denominado "Rede JurisTC's"), do Comitê Técnico de Gestão da Informação (ou rede BIBLIOCONTAS) e da Rede INFOCONTAS (da ATRICON[156]). O resultado dos trabalhos e estudos realizados foram apresentados na Nota Técnica n° 01/2019[157], a qual prevê diretrizes a serem seguidas pelos TC's do Brasil com vistas ao atendimento da LGPD.

A referida nota técnica levou em conta os princípios propugnados na LGPD, quais sejam, o respeito à privacidade; à autodeterminação informativa; à liberdade de expressão, de informação, de comunicação e de opinião; à inviolabilidade da intimidade, da honra e da imagem; ao desenvolvimento econômico e tecnológico e a inovação; à livre iniciativa, livre concorrência e defesa do consumidor e aos direitos humanos e de liberdade e dignidade das pessoas.

As orientações nela contempladas visam padronizar as edições dos atos normativos *interna corporis* que versem sobre as regras de coleta e tratamento de informações de pessoas, órgãos públicos e demais jurisdicionados, os direitos de titulares de dados, as responsabilidades de quem processa esses registros e as estruturas e formas de fiscalização e eventuais reparos em caso de abusos nesta prática, entre outras situações.

Para a emissão de suas orientações, as quais serão levadas em conta no presente trrabalho, o supra citado Grupo de Estudos considerou que, conquanto a aplicação da LGPD tenha reflexos para os Tribunais de Contas tanto na execução de seus processos administrativos internos quanto no desempenho de suas atividades finalísticas (Controle Externo), dever-se-á a sua interpretação e aplicação serem feitas em consonância com o ordenamento jurídico e constitucional existente, sem olvidar nem retroceder em termos de transparência, acesso à informação e publicidade.

2.4 Aparente Conflito entre o direito de acesso à informação e a proteção de dados pessoais

Um aspecto da LGPD a ser considerado na aplicação de seus dispositivos, notadamente quando

---

por este motivo recebeu o slogan de ser "*a casa do conhecimento dos tribunais de contas*". Disponível em: <www.irbcontas.org.br> Acessado em:23 de jan. 2020.

[156] Criada em 16 de agosto de 1992, a Associação dos Membros dos Tribunais de Contas do Brasil (Atricon) atua com o intuito de garantir a representação, a defesa, o aperfeiçoamento e a integração dos Tribunais de Contas e de seus Membros (Ministros, Conselheiros, Ministros Substitutos e Conselheiros Substitutos), visando aprimorar o Sistema de Controle Externo do Brasil em benefício da sociedade. Disponível em: <http://www.atricon.org.br/institucional/apresentacao/> . Acessado em: 23 de jan. de 2020.

[157] Disponível em: <www.irbcontas.org.br> . Acessado em:23 de jan. 2020.

da utilização de dados pessoais pela Administração Pública no Brasil, é a sua interação com a LAI, a qual regulamenta o direito constitucional de acesso às informações públicas. Essa lei entrou em vigor em 16 de maio de 2012 e criou mecanismos que possibilitam, a qualquer pessoa, física ou jurídica, sem necessidade de apresentar motivo, o recebimento de informações públicas dos órgãos e entidades.

Em virtude disso, e diante da constante exigência de transparência quando da utilização de recursos da sociedade na execução das políticas públicas, razão pela qual facilitou-se demasiadamente o acesso a qualquer pessoa, física ou jurídica, ao recebimento de informações públicas dos órgãos e entidades, emergiram-se dúvidas, questionamentos, divergências de opiniões, suscitando um aparente conflito entre o direito de acesso à informação e o direito à proteção de dados pessoais.

Importa ao presente trabalho, em relação a este tópico, apenas discorrer sucintamente acerca da relação entre os diplomas normativos que tratam da proteção de dados e o direito de acesso à informação pelo usuário de serviços públicos, ou mesmo do titular dos dados manuseados/tratados pelo Setor Público, mais precisamente o vínculo entre a LGPD e a LAI no Brasil, posto que o RGPD contemplou em seu bojo todo um regramento o qual preencheu qualquer lacuna porventura alegada durante o processo de aprovação de seu texto final. Tanto é assim, que o direito à informação na ótica do RGPD é considerado um dos direitos mais importantes dos titulares dos dados, eis que permite que estes sejam informados no tocante a todos os dados relevantes sobre o tratamento de dados; quem é o responsável de tratamento; o EPD e seus contactos; as finalidades do tratamento; o prazo de conservação; os direitos do titular e a forma de exercê-los; o momento em que tais informações devem ser tratadas, a depender da presença ou não do titular dos dados.

A transparência dos dados por parte do Poder Público é princípio constitucional que foi regulamentado no Brasil pela LAI e traz como um dos seus limites a vedação ao fornecimento de dados pessoais pelo Poder Público. A composição entre os princípios da proteção de dados pessoais e da transparência é tema que perpassa a regulamentação referente aos dois assuntos, os quais estão, por conseguinte, interligados e com delimitações.

Estas delimitações apresentam-se como necessárias em diversos sistemas jurídicos, a exemplo da UE, cujo Grupo de Trabalho do Artigo 29 (GT 29), em seu parecer sobre os dados abertos e a reutilização de informações do setor público, destacou que o objetivo de se assegurar acesso à informação gerida por órgãos públicos é garantir transparência e controle sobre esses mesmos órgãos. Isto significa que, a despeito de outros objetivos, deve-se ter em conta, precipuamente, os objetivos primários de direitos de acesso à informação, posto que esta têm a ver com a salvaguarda da transparência dos agentes públicos, com o reforço dos controles democráticos. Contudo, a efetividade dessa transparência deve dar-se em consonância com os direitos fundamentais de privacidade e proteção

de dados, sendo este objetivo o que está nas entrelinhas do disposto no Art. 31 da LAI, como forma de garantir esse equilibrio de interesses.

Destarte, como alhures comentado, o Art. 23 do capítulo IV da LGPD, faz menção expressa a LAI, não apenas no caput, mas também nos §§ 2° e 3°,sendo que, neste último traz a exigência de que os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público seguirão as disposições de legislações específicas, entre as quais a retromencionada lei de acesso à informação, ato normativo cujo escopo é regulamentar o direito Constitucional[158] de qualquer pessoa solicitar e receber dos órgãos públicos, em todas as esferas de governo, informações públicas por eles produzidas, de seu interesse particular, ou interesse coletivo ou geral.

Conforme o Art. 4°, inciso I, da LAI, as informações as quais qualquer pessoa têm o direito assegurado no inciso XXXIII do Art. 5° da Constituição Federal, são os dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, registrados em qualquer suporte ou formato. E, ainda, de acordo com o § 3° do Art.10°, da Lei de Acesso à Informação, são vedadas quaisquer exigências relativas aos motivos determinantes da solicitação de informações de interesse público, contudo, em interação com a LGPD, o Órgão Público objeto da solicitação pode verificar junto ao solicitante a melhor forma de atender a demanda, de modo a fornecer a informação mais adequada a sua solicitação.

A Lei de Acesso à Informação contém dispositivos de aplicação imediata a todos os Órgãos Públicos, bem como dispositivos que necessitam de regulamentação específica por cada Poder e Ente da Federação. Ela abrange toda a Administração Direta e Indireta, considerando aqui também as entidades controladas direta ou indiretamente pelos Municípios; as entidades privadas sem fins lucrativos que recebam recursos públicos diretos (do orçamento) ou indiretamente mediante auxílios, contratos de gestão, termo de parceria, convênios, ajustes, acordos ou instrumentos congêneres para a realização de ações de interesse público.

É importante ressaltar que diante das discussões, seminários, congressos etc com vistas à elaboração da LGPD, arrastadas ao longo da última década, os Poderes Públicos Federais, Estaduais e Municipais envidaram esforços no sentido de regulamentarem os procedimentos para a garantia de acesso à informação e para classificação de informações sob restrição. Neste norte, o Poder Executivo Federal publicou o Decreto nº 7.724, de 16 de maio de 2012, alterado pelo Decreto nº 9.960, de 23 de

[158] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado. Disponível em: <www.stf.jus.br/constituição>, Acessado em: 14 de fev. de 2020.

janeiro de 2019, os quais regulam os procedimentos para a garantia do acesso à informação e para a classificação de informações sob restrição de acesso, observados grau e prazo de sigilo, conforme o disposto na LAI, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do Art. 5º, no inciso II do § 3º do Art. 37[159] e no § 2º do Art. 216[160] da CRFB.

Para dar efetividade às disposições tanto da LGPD quanto da LAI, o Poder Executivo Federal produziu uma cartilha intitulada "Guia de Transparência Ativa para Órgãos e Entidades"[161] a qual traz em seu bojo uma compilação de obrigações, elaborado pela Controladoria Geral da União (CGU), cujo objetivo é auxiliar no correto cumprimento das obrigações previstas Lei de Acesso à Informação e demais normas que regem o assunto.

Levando em conta que a LAI estabelece que as informações de interesse coletivo ou geral devem ser divulgadas de ofício pelos órgãos públicos, espontânea e proativamente, independentemente de solicitações, e que em seu art. 8º há a previsão de um rol mínimo de dados que os órgãos e entidades devem, obrigatoriamente, divulgar nas suas páginas oficiais na internet, no menu "Acesso à Informação", a supra citada cartilha, ao padronizar os sites oficiais, facilita a navegação em todos os sites ao tempo em que dá mais agilidade na localização e obtenção das informações desejadas. Segundo consta da Guia de Transparência„"[...] *a divulgação espontânea do maior número possível de informações, além de facilitar o acesso, também é vantajosa porque tende a reduzir as demandas sobre o assunto nos canais de transparência passiva"*[162]*. Tal iniciativa, reduz sobremaneira os trabalhos e os custos de processamento e gerenciamento dos pedidos de acesso, sobretudo quando são tornadas públicas informações, independente de requerimento, utilizando principalmente a Internet, vale dizer, quando a divulgação de dados é feita por iniciativa do próprio setor público, consubstanciando na chamada "transferência ativa*", *e.g.* das seções de acesso a informações dos sites dos órgãos e entidades

---

[159] § 3º A lei disciplinará as formas de participação do usuário na administração pública direta e indireta, regulando especialmente: (Redação da EC 19/1998)
II - o acesso dos usuários a registros administrativos e a informações sobre atos de governo, observado o disposto no art. 5º, X e XXXIII; (Incluído pela EC 19/1998)

[160] Art. 216. Constituem patrimônio cultural brasileiro os bens de natureza material e imaterial, tomados individualmente ou em conjunto, portadores de referência à identidade, à ação, à memória dos diferentes grupos formadores da sociedade brasileira, nos quais se incluem:
§ 2º Cabem à administração pública, na forma da lei, a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem. Disponível em: <www.stf.jus.br/constituição>, Acessado em: 14 de dez. de 2019.

[161] Guia de Transparência Ativa para Órgãos e Entidades do Poder Executivo Federal - 6ª Versão – 2019. Disponível em: <www.acessoainformacao.gov.br/lai-para-sic/guias-e-orientacoes/gta-6a-versao-2019.pdf>. Acessado em: 22 de dez. de 2019.

[162] É a disponibilização de informações públicas em atendimento a demandas específicas de uma pessoa física ou jurídica. Por exemplo, a resposta a pedidos de informação registrados para determinado Ministério, seja por meio do SIC físico do órgão ou pelo e-SIC (Sistema Eletrônico do Serviço de Informação ao Cidadão). Disponível em: <http://www.acessoainformacao.gov.br>. Acessado em 23 de dez. de 2019.

e dos portais de transparência.

A par disso, e ante a necessidade de complementar a LGPD, o Poder Executivo Federal do Brasil publicou o Decreto nº 10.046/2019, de 9 de outubro de 2019, o qual estabeleceu normas e diretrizes para o compartilhamento de dados entre os órgãos e entidades da administração pública direta, autárquica e fundacional e os demais Poderes da União. O retrocitado Decreto, que atua em caráter complementar à Lei nº 13.709/18 – "LGPD", define alguns atributos a serem considerados como dados pessoais compartilhados e estabelece os níveis de compartilhamento de dados pessoais no âmbito da administração pública federal, a partir do grau de confidencialidade dos dados que estão sob o controle do Poder Público. É com base nessas definições que serão estabelecidas regras específicas de compartilhamento e medidas de segurança para as transferências de dados.

Ademais, o Decreto instituiu o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados com duas finalidades específicas, a saber: enquanto o primeiro tem a finalidade de criar uma base de dados integradora única, em formato interoperável, com capacidade de disponibilizar diversas informações pessoais dos cidadãos aos órgãos e entidades do Poder Executivo Federal, o segundo, trata-se de órgão deliberativo, cujas competências abrange, entre outras, o estabelecimento de diretrizes e regras para as diferentes categorizações de compartilhamento - amplo, restrito e específico; a compatibilidade de políticas de segurança da informação e as comunicações realizadas pelo órgãos e entidades; a forma de avaliação da integridade, da qualidade e da consistência de base de dados derivadas da integração de diferentesa bases de dados com o Cadastro Base do Cidadão; a resolução de controvérsias sobre a validade de informações cadastrais e as regras de prevalência entre eventuais registros administrativos conflitantes, no caso de cruzamento de informações entre bases de dados do Cadastro Base; a inclusão, na base integradora do Cadastro Base do Cidadão, de novos dados provenientes das bases temáticas, considerada a eficiência técnica e a economicidade; a instituição de outros cadastros base de referência do setor público de uso obrigatório pelos órgãos e entidades.

Há algumas questões a serem ponderadas resultante de uma breve análise do Decreto 10.046/2019. É cediço que a LGPD entrará em vigor em agosto de 2018, e, pelo Decreto, foi conferido um prazo de 90 (noventa) dias, a contar da data de publicação, para que os órgãos federais pudessem categorizar os dados em restrito ou específico, levando em conta que a categorização dos tipos de compartilhamento dos dados deve ser em níveis compatíveis com a sensibilidade da informação.

Com a criação do Cadastro Base do Cidadão, o Poder Executivo pretendeu evitar o deslocamento dos cidadãos a órgãos públicos para obtenção de documentos e certidões, e concentrou os dados numa única fonte de informações dos cidadãos com o Poder Público, a partir de dados disponíveis no Cadastro de Pessoa Física, tais como o número do CPF, o nome completo, a data de nascimento, o

sexo, a filiação, a nacionalidade, além de outros atributos biográficos e cadastrais, à exceção dos dados protegidos por sigilo fiscal, que estão sob controle da RFB.

O aludido cadastro compõe-se de dados cadastrais, dados biográficos e dados biométricos – daí excetuando-se os "atributos genéticos", qual seja, o DNA. Neste aspecto, há divergências conceituais, posto que a LGPD fala em "dados pessoais" e "dados pessoais sensíveis", já o decreto classifica os dados dos cidadãos em "cadastrais", "biográficos", "biométricos" e "atributos genéticos". Segundo a Lei Geral de Proteção de Dados, origem étnica, opinião política, genética e biometria de uma pessoa são dados considerados sensíveis e requerem um tratamento especial por parte dos órgãos públicos e demais Entidades. Por outra banda, vimos que o decreto estabelece três categorias de compartilhamento para os dados na esfera pública (amplo, restrito e especifico), cabendo ao gestor dos dados a classificação. Há de se buscar a conciliação conceitual.

No tocante ao Comitê Central de Governança de Dados (CCGD), verifica-se que o Decreto estabelece a sua constituição apenas por representantes indicados pelo Executivo Federal, contudo a LGPD, após as alterações introduzidas pela Lei n° 13.853, de 8 de julho de 2019, estabeleceu a criação da ANPD, composta por um conselho diretor com cinco membros, todos indicados pelo presidente da República, vedada a demissão após nomeados, com funções de regulação e fiscalização do cumprimento da lei. Neste contexto, verifica-se uma sobreposição de atribuições entre ANPD e CCGD, o que poderia ter sido evitado, uma vez que a criação da Autoridade Nacional precede a criação do Comitê Central. É uma questão a ser conciliada, posto que a previsão de início de vigência da LGPD em sua integralidade remonta a meados de 2020, considerando o disposto no inciso II do Art. 65 da Lei 13.853/2019[163].

Estas aparentes incongruências entre os dispositivos das legislações supraevidenciadas provocaram reações doutrinárias positivas e negativas, senão vejamos. Segundo Flávia Lefèvre[164], *"o Decreto 10.046 é uma iniciativa no mínimo surpreendente porque acabamos de aprovar a LGPD, que entra em vigor em menos de um ano e que contempla expressamente os poderes públicos. Eu esperava que essa questão de transferência de dados entre órgãos públicos fosse regulamentada pela ANPD. Em certa medida esse decreto esvazia a atribuição da ANPD"*.

[163] Art. 65. Esta Lei entra em vigor:

II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos.

[164] Cfe. Flávia Lefèvre Guimarães - advogada especializada em direito do consumidor, telecomunicações e direitos digitais. É integrante da Coalizão Direitos na Rede e consultora associada do Instituto NUPEF - Núcleo de Pesquisas, Estudos e Formação; foi representante das entidades de defesa do consumidor no Conselho Consultivo da ANATEL de fevereiro de 2006 a fevereiro de 2009 e recentemente eleita para representar o 3º Setor no Comitê Gestor da Internet no Brasil (2014 a 2020). Disponível em: <https://flavialefevre.com.br/pt/about>. Acessado em: 23 de dez. de 2019.

A seu turno, Rafael Pellon[165], especializado em direito digital, vê como positivo o esforço de digitalização do governo federal e de unificação de dados de cidadãos beneficiados por programas sociais, conquanto entenda que o Decreto 10.046 faça isso à margem da LGPD, sem observar várias das disposições da lei. Em sua visão, "[...] *o ideal seria que o governo criasse um grande portal do cidadão, onde este pudesse exercer seus direitos previstos na LGPD, como a visualização, a atualização, a retificação ou mesmo a exclusão dos seus dados. O governo guardaria aqueles que fossem essenciais para políticas públicas e programas sociais".*

Afora as questões aqui levantadas, convém destacar as mudanças de ordem prática a serem provocadas pelo Decreto 10.046/2019, uma vez que, como visto, além de facilitar o acesso aos serviços públicos, o cadastro unificado ajudará a subsidiar e monitorar as políticas públicas, o que terá implicações positivas na análise de condições para acesso aos benefícios sociais e fiscais e sua respectiva manutenção, bem como promoverá a melhoria da qualidade dos dados sob gestão do governo federal e incrementará a eficiência das operações internas dos órgãos e entidades a ele subordinados.

Destarte, em relação aos cidadãos no exercício de seu direito de acesso aos dados e obtenção de informações que lhes digam respeito, se antes havia a necessidade de reunir documentos de diversos órgãos, e.*g* de certidões, comprovantes de situação fiscal e cadastral entre outros, para o cumprimento de seus deveres cívicos, com a integração entre os órgãos proposta pelo Decreto, a entrega de documentos e certidões para solicitar um serviço passará a ser facilitada e simplificada; se antes as regras não garantiam a segurança necessária para um efetivo compartilhamento de dados entre os órgãos, o Decreto trouxe regras mais claras em relação a isto, acelerando a troca de informações e, concomitantemente, garantindo a proteção dos dados do cidadão e promovendo ainda mais transparência, proteção e facilidade na negociação e consequente tramitação de informações entre os Órgãos e Entidades Públicos.

CAPÍTULO III – Quesitos de proteção de dados

Seguindo a estrutura até então desenvolvida, e considerando essencialmente as regras do RGPD e da LGPD atinentes à necessária segurança exigida para o compartilhamento de dados entre os Órgãos e Entidades Públicos, que garantam ao mesmo tempo a proteção dos dados dos cidadãos, sem prejuízo da observância dos Princípios da Legalidade, Transparência e Publicidade na aplicação dos recursos públicos, buscar-se-á apresentar o nível de envolvimento de um dos Órgãos Constitucionais responsável pelo tratamento de dados que lhes são enviados pelas Entidades por eles fiscalizadas no

[165] Cfe. Rafael Pellon de Lima Sampaio – advogado especialista em Telecomunicações, Internet, Mídia e Entretenimento. Disponível em: <https://www.jusbrasil.com.br/topicos/29291674/rafael-pellon-de-lima-sampaio>. Acessado em: 23 de dez. de 2019.

exercício do cumprimento de sua função primordial.

A referência que ora se faz é aos Tribunais de Contas, sendo que, para o escopo do presente trabalho, como já alhures discriminado, o campo de análise limitar-se-á ao Tribunal de Contas do Rio Grande do Norte e ao Tribunal de Contas da Paraíba, ambos com juridição no Brasil, e ao Tribunal de Contas de Portugal.

De início, é de bom alvitre salientar que as respectivas Constituições, do Brasil e de Portugal, coloca-os em posições hierárquicas distintas, a saber: enquanto a Constituição de Portugal, em seu Art. 110, eleva o Tribunal de Contas de Portugal ao status de Órgão de Soberania[166], a Constituição da República Federativa do Brasil confere aos seus Tribunais de Contas a condição de meros órgãos auxiliares do Poder Legislativo[167] no exercício do controle externo o que, frise-se desde logo, representa uma desvantagem na imposição do cumprimento de suas decisões prolatadas pelos respectivos colegiados.

Isto posto, interessa-nos perquirir o nível de interação existente entre as lesgislações *interna corporis* do TC. de Portugal e o RGPD, ou por existir, no caso dos Tribunais de Contas do Brasil supra evidenciados, sem pretensão de se esgotar um tema que está em constante desenvolvimento.

A motivação por enveredar neste aspecto foi reforçada sobretudo pela observação realizada *in loco,* na qual se constatou sob diferentes manifestações o grau de envolvimento dos servidores e membros dos TC's acerca dos diplomas normativos referentes à proteção de dados pessoais. Explicando melhor, despertou curiosidade, especialmente nos dois TC's do Brasil pesquisados, a distância a ser percorrida pela área da Tecnologia de Informação para alçar a condição de estar ao alcance do que propõe a LGPD, seja pela falta de conhecimento da própria lei, seja pela incipiente canalização de esforços e recursos humanos e materiais necessários para tornar o ambiente interno adequado às exigências da legislação. Neste ponto, vale salientar que o TC. de Portugal está em um patamar que serve de referencial, como poderá ser constatado ao longo das próximas linhas.

Para obter-se um parâmetro de análise, partiu-se de um referencial teórico buscado em alguns diplomas normativos que precederam a elaboração das respectivas legislações sobre proteção de dados pessoais. Com base no dito referencial, elaborou-se um questionário dirigido a alguns funcionários dos TC's do Brasil, a fim de se obter informações que permitissem aferir não apenas o grau de

[166] Art. 110

(Órgãos de soberania)

1. São órgãos de soberania o Presidente da República, a Assembleia da República, o Governo e os Tribunais.

[167] Art. 71. O controle externo, a cargo do Congresso Nacional, será exercido com o auxílio do Tribunal de Contas da União, ao qual compete: Disponível em: <www.stf.jus.br/constituição>, Acessado em: 28 de dez. de 2019.

envolvimento, interesse, participação e importância das regras relativas à proteção de dados pessoais para a escorreita atuação destas Entidades, como também, e principalmente, atestar se é do conhecimento de todos a existência de uma Lei Geral de Proteção de Dados.

A título de exemplificação, acerca das expectativas e da aparente desinformação "pairada no ar", optou-se por iniciar o questionário buscando uma informação básica, porém respaldada nas próprias legislações civis do Brasil e de Portugal. Com efeito, assim dispõe a LINDB, em seu art. 3°: "*Ninguém se escusa de cumprir a lei, alegando que não a conhece"*. Similarmente, o CC. de Portugal, ao disciplinar sobre a conduta do cidadão relativamente ao conhecimento das leis, prescreve em seu art. 6°: *"A ignorância ou má interpretação da lei não justifica a falta do seu cumprimento nem isenta as pessoas das sanções nela estabelecidas"*

Como se percebe, tanto a legislação portuguesa quanto a brasileira, com base no princípio iluminista, estatui que a ignorância da lei não aproveita a ninguém, ou seja, há um pressuposto de que existe um dever de conhecer a lei do Estado, a qual é de natureza pública. Convém frisar que a própria evolução da tecnologia da Informação tornou mais fácil e rápido o acesso do cidadão aos inúmeros conteúdos das legislações, por meio de diversas ferramentas de acesso, o que não justificaria de modo algum o desconhecimento ou a ignorância do agente público acerca das leis.

Os questionários aplicados foram divididos em dois grupos, sendo o primeiro deles, dirigido aos servidores do Tribunal de Contas da Paraíba e ao Tribunal de Contas do Rio Grande do Norte, composto de 18 (dezoito) perguntas encabeçadas por 8 temas. O segundo questionário abrangeu quatro temas e 13 perguntas, as quais foram pessoalmente formuladas ao Chefe do DSTI do Tribunal de Contas de Portugal. Pretendeu-se, com os referidos questionários, obter uma visão geral do estágio de adequação das normas internas dos referidos Tribunais de Contas aos ditames das respectivas legislações nacionais sobre proteção de dados. Não se buscou um grau de aprofundamento condizente com todos os temas trazidos a cabo pela LGPD e pelo RGPD e, sim, contribuir para que fosse ampliada a consciência do dever de participação dos funcionários dos Tribunais de Contas como agentes ativos na implementação em concreto das regras contidas nos retrocitados atos normativos.

As respostas obtidas em muito contribuiram não apenas para aferir o nível de adequação dos respectivos sistemas de acompanhamento de gestão às regras de proteção de dados pessoais, mas, também, para as observações e sugestões finais objeto de conclusão do presente trabalho, no sentido de poder contribuir para a melhoria da eficiência de sua aplicação nos sistemas destes Tribunais de Contas, precipuamente os do Brasil. Isto porque a excelência de um sistema de acompanhamento de gestão não pode prescindir dos princípios norteadores da proteção de dados pessoais.

Saliente-se que se optou por perguntas objetivas, por não se identificar os participantes e,

precipuamente, por trazer um conteúdo o mais próximo possível das atividades desenvolvidas no âmbito dos Tribunais de Contas contemplados. Ademais, os questionários prestaram-se a nortear a pesquisa e observação realizada *in loco* e o desenvolvimento da presente dissertação.

Nas linhas que se seguem, apresentam-se os questionários propostos com as perguntas e a fundamentação legal e, na sequência, a apresentaçãqo dos resultados obtidos, tendo-se em conta, vale repisar, a distância existente entre o TC. de Portugal e os TC's do Brasil no que diz respeito aos estudos de adequação às regras de proteção de dados pessoais existentes nas respectivas legislações.

QUESTIONÁRIO APLICADO AO TCE/ RN E TCE/ PB

TEMA	PERGUNTA	BASE LEGAL
GERAL	1– É do conhecimento do Órgão Público/servidor público a existência de uma legislação cujo objeto é o tratamento de dados pessoais?	Art. 3º, da Lei nº 12.376/10; Art.1° da Lei nº 13.709/18
	2 - O Órgão Público possui ferramenta de pesquisa de conteúdo que permita o acesso à informação?	Art. 5º, XXXIII c/c o Art. 3º inciso II, com o Art. 216, § 2º , com o art. 37, § 3°, inciso II Constituição - Federal; Art. 6° c/c Art. 8º, §3º, I, da Lei 12.527/11;
INFORMAÇÃO	3 – Para os efeitos de tratamento legal, é claro para o servidor público o conceito e os tipos de informação manuseadas pela área de Tecnologia da Informação?	Art. 4° da Lei 12.527/11; Art. 5º da Lei nº 13.709/18
DADOS	4 - Para os efeitos de tratamento legal, é claro para o servidor público o conceito e os tipos de dados manuseados pela área de Tecnologia da Informação?	Art. 5º da Lei nº 13.709/18; Art. 4° da Lei 12.527/11;
	5 – O banco de dados está concentrado na área de Tecnologia da Informação ou está distribuído em vários locais do Órgão Público?	
TRATAMENTO DE DADOS	6 – Os servidores titulares de dados são previamente informados acerca da finalidade para a qual seus dados são tratados?	Art. 6º c/c Art. 7° e o Art. 9°; o Capítulo IV da Lei nº 13.709/18
	7 – É garantido o livre acesso bem como a integralidade dos dados pessoais aos seus titulares?	
	8 – Há utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais autorizados e não autorizados e de situações acidentais ou ilícitas de destruição, perda etc?	

	9- Existe algum estudo ou mesmo ferramenta no sentido de garantir o prévio consentimento do titular para que os seus dados sejam tratados, inclusive quanto aos dados pessoais sensíveis? 10 – Existe um encarregado pelas operações de tratamento de dados pessoais? 11 – Em seu sítio eletrônico, há alguma informação clara e atualizada acerca da previsão legal, da finalidade e dos procedimentos e práticas utilizadas no tratamento de dados pessoais?	
COMPARTILHAMENTO DE DADOS	12 - O Órgão compartilha dados pessoais com terceiros? Observadas as hipóteses: • Para execução descentralizada de atividade pública • Em virtude de contratos, convênios ou de previsão legal • Para prevenção de fraudes e irregularidades ou para proteger e resguardar a segurança e integridade do titular dos dados • No caso dos dados serem acessíveis publicamente aos solicitantes.	Art. 26, caput, e § 1° da Lei nº 13.709/18; Art. 7° da Lei nº 12.527/11
PUBLICAÇÃO DE RELATÓRIO/ACESSO À INFORMAÇÃO	13 - O Site do Órgão possibilita a gravação de relatórios em diversos formatos eletrônicos, abertos e não proprietários, tais como planilhas e texto (CSV), de modo a facilitar a análise das informações? 14 – O site possibilita a obtenção de informações relativas à: • Administração do patrimônio público, utilização de recursos públicos, licitação, contratos administrativos? • Ao resultado de inspeções, auditorias, prestação e tomadas de contas realizadas em seus jurisdicionados?	Art. 32. da Lei nº 13.709/18; Art. 7° e Art. 8° da Lei nº 12.527/11

APLICAÇÃO EM CONCRETO DA LGPD NAS ATIVIDADES JURISDICIONAIS	15 – Nos processos de Auditoria, constam apenas as informações relevantes diretamente relacionadas com o objeto e âmbito da auditoria, preservando-se os dados pessoais? 16 – Nos processos de denúncia, há a proteção dos dados pessoais do denunciante e denunciado até a decisão definitiva de mérito? 17 – Nos processos de Consulta dos Relatórios dos órgãos de controlo interno que contenham dados pessoais, são assegurados procedimentos de segurança ou até mesmo restrição do acesso à informação? 18 – Ao publicar as suas decisões, o Tribunal de Contas tem observado as regras de limitação e conservação dos dados pessoais, que permitem a identificação de seus titulares, atendendo apenas ao período necessário as finalidades para as quais são tratados?	Art. 5°, Art. 25°, n° 2 do RGPD; Art. 19. Alínea c) e Art. 142° do Regulamento 112/2018 de 15 de fevereiro. OBS: aplicado por similaridade de atribuições ao TC/RN e ao TC/PB

QUADRO 3 **FONTE: DO AUTOR**

As respostas obtidas não apresentaram uma avaliação positiva na relação entre funcionários e o conhecimento da LGPD, como poderá ser verificado pelos números levantados a seguir. Os gráficos levantados estão agrupados nos anexos desta dissertação e a análise do resultado apresenta apenas os percentuais das respostas relevantes, deduzindo-se que a parte não relevante corresponde aos que responderam em sentido oposto ao apresentado.

De um universo pretendido de 32, responderam ao questionário 25 funcionários ocupantes de cargos de chefia do TCE/RN e do TCE/PB, o que corresponde a aproximadamente 80%, sendo considerado suficiente para se chegar a algumas conclusões, notadamente pelo fato de que aquelas chefias refletem o pensamento de seus subordinados em relação ao tema LGPD.

Das duas perguntas de ordem geral, observou-se que apenas 68% têm conhecimento da LGPD, ou seja, sabem que foi aprovada uma lei de proteção de dados pessoais, contudo, 88% sabem que o Órgão em que trabalham dispõe de ferramenta de pesquisa que permite o acesso à informação. Por outro lado, ao serem indagados acerca dos tipos de informação e dados tratados pela área de TI, somente 24% e 16%, respectivamente, afirmaram ter conhecimento.

Em relação armazenamento dos dados recolhidos, 48% tem a informação de que o banco de dados está concentrado na área de TI. Quanto ao tratamento de dados, 48% disseram que são previamemte informados acerca da finalidade para a qual seus dados são tratados; 64% afirmam ser garantido o livre acesso bem como a integralidade de seus dados pessoais; 52% tem conhecimento de que há utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais; 80% disseram que não existe, ou não sabem informar com precisão, algum estudo ou mesmo ferramenta no

sentido de garantir o prévio consentimento do titular para que os seus dados sejam tratados, inclusive quanto aos dados pessoais sensíveis; 70% não sabem informar se há, ou afirmam não existir, um ecarregado pelas operações de tratamento de dados; 84% disseram que não sabem informar se existe, ou afirmam não existir, no sítio eletrônico do Tribunal, informação clara e atualizada acerca da previsão legal, da finalidade e dos procedimentos e práticas utilizadas no tratamento de dados pessoais.

Relativamente ao compartilhamento de dados pessoais com terceiros, foram obtidas as seguintes respostas: 44% responderam que os TC's compartilham dados para a execução descentralizada de atividade pública; 56% responderam que os TC's compartilham dados em virtude de contratos, convênios ou de previsão legal; 32% responderam que os TC's compartilham dados para prevenção de fraudes e irregularidades ou para proteger e resguardar a segurança e integridade do titular dos dados; e 36% responderam que os TC's compartilham dados no caso dos dados serem acessíveis publicamente.

No tocante à publicação de relatório/acesso à informação, assim se responderam: 72% disseram que os TC's possibilitam a gravação de relatórios em diversos formatos eletrônicos, abertos e não proprietários, tais como planilhas e texto (CSV), de modo a facilitar a análise das informações; 88% responderam que o sítio eletrônico possibilita a obtenção de informações relativas à administração do patrimônio público, utilização de recursos públicos, licitação, contratos administrativos; e 92% responderam que o sítio eletrônico possibilita a obtenção de informações relativas ao resultado de inspeções, auditorias, prestação e tomadas de contas realizadas em seus jurisdicionados.

No que diz respeito aos Processos do Tribunal de Contas: 44% responderam que, nos processos de Auditoria, constam apenas as informações relevantes diretamente relacionadas com o objeto e âmbito da auditoria, preservando-se os dados pessoais; 40% responderam que, nos processos de denúncia, há a proteção dos dados pessoais do denunciante e denunciado até a decisão definitiva de mérito; 28% responderam que, nos processos de Consulta dos Relatórios dos órgãos de controlo interno que contenham dados pessoais, são assegurados procedimentos de segurança ou até mesmo restrição do acesso à informação; 48% responderam que, ao publicar as suas decisões, o Tribunal de Contas tem observado as regras de limitação e conservação dos dados pessoais, que permitem a identificação de seus titulares, atendendo apenas ao período necessário às finalidades para as quais são tratados.

O questionário aplicado ao TC. de Portugal, diferentemente daquele dirigido aos TC's do Brasil, tem o objetivo tão somente de atestar a conformidade das ações já em andamento com os requisitos do RGPD. Desta forma, o questionário foi encaminhado apenas ao setor responsável pelo desenvolvimento de ferramentas de tecnologia da Informação e demais atribuições correlatas, o DSTI, cujas atividades são de amplo escpectro, vale dizer, contempla ferramentas de TI que se prestam à comunicação tanto internamente quanto externamente, cujas informações são acessíveis também aos

cidadãos. As perguntas foram feitas pessoalmente ao Diretor Geral do TC. de Portugal, bem como ao Chefe do DSTI.

QUESTIONÁRIO APLICADO AO DSTI DO TRIBUNAL DE CONTAS DE PORTUGAL

TEMA	PERGUNTA	BASE LEGAL
GERAL	1– O servidor público está ciente de que o Tribunal de Contas de Portugal tem realizado estudos que objetivam assegurar o cumprimento dos dispositivos legais do RGPD em seu ambiente interno?	Art. 13° e Art. 19°, nº 2, alínea c) do Regulamento 112/2018, de 15 de fevereiro; Art. 2°, n° 3, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho; Art. 1° do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho.
	2 – Dos estudos realizados, o Tribunal de Contas de Portugal tornou efetiva a adoção das medidas inicialmente planejadas? Quais sejam: 2.1- A adequação da publicitação do conteúdo dos atos do Tribunal ao princípio da minimização de dados; 2.2 - A designação de um Encarregado da Proteção de Dados e a definição de seu estatuto.	RESOLUÇÃO N° 3/2018-PG do Tribunal de Contas de Portugal; Arts. 37°, 38° e 39°-Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho; Art. 43°- Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho; GT29 da Diretiva 95/46/CE.
DADOS	3 - Para os efeitos de tratamento legal pelo RGPD é claro para o servidor público o conceito e os tipos de dados manuseados pela área de Tecnologia da Informação? 4 – O banco de dados está concentrado na área de Tecnologia da Informação ou está distribuído em vários locais do Tribunal de Contas?	Art. 4º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho; Art. 3° do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho.
TRATAMENTO DE DADOS	5 – Os titulares de dados, sejam eles servidores ou jurisdicionados do Tribunal de Contas são previamente informados acerca da finalidade para a qual seus dados são tratados? 6 – É garantido o direito de acesso bem como a integralidade dos dados pessoais aos seus titulares? 7 – Há utilização de medidas técnicas e organizativas aptas a proteger os dados pessoais autorizados e não autorizados e de situações acidentais ou ilícitas de destruição, perda etc? 8 - Existe algum estudo ou mesmo ferramenta no sentido de garantir o prévio consentimento do titular para que os seus dados sejam tratados, inclusive quanto aos dados pessoais sensíveis? 9 – No sítio eletrônico do Tribunal de Contas, há alguma informação clara e atualizada acerca da previsão legal, da finalidade e dos procedimentos e práticas utilizadas no tratamento de dados pessoais?	Art. 5°; Art. 6º, alíneas c) e e); Art. 7°; Art. 9°; Art. 32° do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho; Considerando 20 do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho; GT29 da Diretiva 95/46/CE.

APLICAÇÃO EM CONCRETO DO RGPD NAS ATIVIDADES JURISDICIONAIS	10 – Nos processos de Auditoria, constam apenas as informações relevantes diretamente relacionadas com o objeto e âmbito da auditoria, preservando-se os dados pessoais? 11 – Nos processos de denúncia, há a proteção dos dados pessoais do denunciante e denunciado até a decisão definitiva de mérito? 12 – Nos processos de Consulta dos Relatórios dos órgãos de controlo interno que contenham dados pessoais, são assegurados procedimentos de segurança ou até mesmo restrição do acesso à informação? 13 – Ao publicar as suas decisões, o Tribunal de Contas tem observado as regras de limitação e conservação dos dados pessoais, que permitem a identificação de seus titulares, atendendo apenas ao período necessário as finalidades para as quais são tratados?	Art. 5°, Art. 25°, n° 2 do RGPD; Art. 19. Alínea c) e Art. 142° do Regulamento 112/2018 de 15 de fevereiro

QUADRO 4 **FONTE: DO AUTOR**

Em atenção às perguntas formuladas, a Direção-Geral e o DSTI responderam aos itens questionados afirmativamente, à exceção das perguntas n° 8 e n° 9, posto que os técnicos estão a desenvolver as ferramentas necessárias. Um outro ponto que foi salientado, refere-se ao banco de dados, eis que este está concentrado na área de Tecnologia da Informação. No tocante as demais perguntas, o conteúdo das respostas estão inseridos no corpo deste trabalho, notadamente nos capítulos dedicados às normas e ao sistema de gestão da informação do TC. de Portugal, respectivamente. Não está evidenciada, portanto, análise referente às respostas obtidas.

Uma vez analisadas as respostas dos questionários, reforçado sobretudo pela observação realizada *in loco,* na qual se constatou sob diferentes manifestações o grau de envolvimento dos funcionários dos Tribunais de Contas acerca dos diplomas normativos referentes à proteção de dados pessoais passar-se-á a perquirir o nível de interação existente entre as lesgislações *interna corporis* do TC. de Portugal e o RGPD, bem como o dos TC's do Brasil e o LGPD.

3.1 O TCE/RN x Proteção de Dados Pessoais

Pelo princípio da simetria, aplicam-se, no que couber, as normas estabelecidas na Constituição Federal para a organização, composição e fiscalização dos Tribunais de Contas do Brasil. É o que prescreve o Art. 75 da Constituição Federal, *in verbis*: *"As normas estabelecidas nesta seção aplicam-se, no que couber, à organização, composição e fiscalização dos Tribunais de Contas dos Estados e do Distrito Federal, bem como dos Tribunais e Conselhos de Contas dos Municípios"*. E o parágrafo único

complementa o aludido artigo ao estabelecer que "*as Constituições estaduais disporão sobre os Tribunais de Contas respectivos, que serão integrados por sete Conselheiros".*

Por sua vez, o Art. 53[168] e o Art. 56[169] da Constituição do Estado do Rio Grande do Norte em atenção à CRFB prescrevem que o controle externo, a cargo da Assembleia Legislativa, é exercido com o auxílio do Tribunal de Contas do Estado, o qual tem sede na Capital, quadro próprio de pessoal e jurisdição em todo o território estadual, em respeito ao Princípio Federativo. exercendo as seguintes atribuições administrativas, além de outras conferidas em lei:

A Lei Orgânica do TCE/RN, bem como o seu Regimento Interno, praticamente não tratam de modo explícito em seus textos acerca da Proteção dos Dados que lhes estão custodiados, digam eles respeito aos informes dos jurisdicionados ou mesmo os relativos aos seus servidores. Contudo, com a inserção do Brasil entre os países que adotaram legislação específica para proteção dos dados e da privacidade de seus cidadãos, a qual determina que todos os dados pessoais - leia-se a informação relacionada à pessoa natural identificada ou identificável, como nome, idade, estado civil, documentos etc - só podem ser coletados mediante o consentimento do usuário, com fundamento em diversos princípios nela elencados, os Tribunais de Contas, a exemplo do TCE/RN, fazendo uso de sua competência interna de legislar sobre sua estrutura e organização de seus serviços, têm buscado adequar estes às inovações trazidas pela Lei Geral de Proteção de Dados.

Tal iniciativa do TCE/RN tem ocorrido de forma pontual e não se mostra eficazmente adequada em sua inteireza à LGPD, havendo apenas uma precaução no sentido de não se extrapolar ou dar uma interpretação além do que permite a Lei de Acesso à Informação, notadamente para se fazer cumprir os Princípios da Transparência e da Publicidade, sem prejuízo da preservação da privacidade dos dados pessoais coletados e armazenados em sua base de dados. Convém, entretanto, comentar em breves linhas o que traz a Lei Orgânica e o Regimento Interno em seus conteúdos para aferir o quanto se

---

[168] Art. 53. O controle externo, a cargo da Assembleia Legislativa, é exercido com o auxílio do Tribunal de Contas do Estado, ao qual compete:

[...] Disponível em: <https://arearestrita.tce.rn.gov.br/as/Legislacao_site/download/constituicoes/CE_RN.pdf>. Acessado em: 24 de fev. de 2020.

[169] Art. 56. O Tribunal de Contas do Estado tem sede na Capital, quadro próprio de pessoal e jurisdição em todo o território estadual exercendo as seguintes atribuições administrativas, além de outras conferidas em lei:

I - eleger seu presidente e demais titulares de sua direção, para mandato de dois (2) anos;

II - elaborar seu regimento interno e organizar os respectivos serviços auxiliares; (grifo nosso)

III - propor ao Poder Legislativo sua lei orgânica, a criação ou a extinção de cargos em seus serviços auxiliares e a fixação dos vencimentos de seus membros e demais servidores.

Disponível em: <https://arearestrita.tce.rn.gov.br/as/Legislacao_site/download/constituicoes/CE_RN.pdf>. Acessado em: 24 de fev. de 2020.

há de fazer para por o TCE/RN em sintonia com a LGPD.

A LCE n° 464, de 5 de janeiro de 2012, com as alterações promovidas pela LCE n° 531, de 12 de janeiro de 2015, denominada Lei Orgânica, é a norma legal que dispõe sobre a natureza, competência e jurisdição do TCE/RN, ao passo que a Resolução n° 009/2012 – TCE é o ato normativo interno que dispõe sobre a aprovação do Regimento Interno do Tribunal de Contas do Estado do Rio Grande do Norte. Por outro lado, o Art. 1° da Lei Complementar Estadual n.º 411[170], de 8 de janeiro de 2010, indica que "o*s serviços técnicos e administrativos necessários ao desempenho da função institucional do Tribunal, compreendem os órgãos de controle externo, administrativos e de assessoramento"* E o inciso X do parágrafo único do mesmo artigo insere oficialmente a Diretoria de Informática como unidade administrativa integrante da estrutura organizacional do Tribunal[171].

Em seu art. 10°, a retromencionada Lei Complementar Estadual n.º 411, de 8 de janeiro de 2010, a qual dispõe sobre a estrutura organizacional do Tribunal de Contas do Estado do Rio Grande do Norte, refere-se à Diretoria de Informática nos seguintes termos: "*A Diretoria de Informática, dirigida por um Diretor, símbolo CC-2, subordinada à Secretaria Geral do Tribunal, tem por finalidade o planejamento, coordenação, execução e supervisão de diretrizes, normas e procedimentos que orientem e disciplinem a utilização dos recursos relacionados à tecnologia da informação, além de outras que lhe forem compatíveis, conferidas por regulamento"*

A seu turno, em seu RI, cujo escopo é o detalhamento das atribuições e demais procedimentos que lhes são atribuídos, o TCE/RN refere-se à Diretoria de Informática apenas uma única vez, mormente ao tratar da prescrição da ação punitiva do Tribunal, no § 2º do art. 328 do título VII*, in verbatim*: "c*aberá à Diretoria de Informática, por meio do portal do Tribunal, alertar os órgãos de controle externo quando da permanência dos processos no mesmo setor por prazo superior a seis meses"*

Isto significa que o TCE/RN remete a matéria relativa à disciplina do planejamento, coordenação, execução e supervisão de diretrizes, normas e procedimentos que orientem e disciplinem a utilização dos recursos relacionados à tecnologia da informação, além de outras que lhe forem compatíveis, à edição de ato normativo interno, infralegal, vale dizer, uma resolução, ou mesmo portaria, a depender da matéria a ser regulamentada.

Neste norte, o TCE/RN publicou a Resolução n° 31/2012 – TCE por meio da qual instituiu o Planejamento Estratégico da Tecnologia da Informação e Plano Diretor de Tecnologia da Informação do

[170] A Lei Complementar nº 411/2010 dispõe sobre a estrutura organizacional do Tribunal de Contas do Estado do Rio Grande do Norte e dá outras providências. Disponível em: <www.tce.rn.gov.br/as/dowload/legislação/LCE_4112010.pdf> . Acessado em: 27 de fev. 2020.

[171] Cfe. texto integral da Lei Complementar nº 411/2010. Disponível em: <www.tce.rn.gov.br/as/dowload/legislação/LCE_4112010.pdf> . Acessado em: 27 de fev. 2020.

TCE/RN para o período de 2012 a 2017, cuja vigência deu-se a partir de 04 de dezembro de 2012. Por meio deste instrumento normativo interno e do referencial estratégico nele estabelecido, a Diretoria de Informática do Tribunal, com a contribuição das demais unidades gerenciais do Órgão, assumiu a responsabilidade pela execução, acompanhamento e avaliação das ações e projetos relativamente a sua área de atuação, conforme previsto no aludido art. 10°, da Lei Complementar Estadual n.º 411, de 8 de janeiro de 2010.

Seguindo o estabelecido no Planejamento Estratégico, os diversos setores do TCE/RN dedicaram-se a implementar as ações nele contempladas visando a melhoria da qualidade de suas atribuições. Nesta mesma linha, também a área de Tecnologia da Informaçãonão dedicou-se a incrementar as ações que lhes cabiam e, entre elas, as que guardam relação com a proteção de dados, levando em conta que, com a iminente entrada em vigor da LGPD do Brasil, emerge necessariamente uma adequação das ações e projetos da área de tecnologia e informação do TCE/RN.

Vale salientar que o aludido Planejamento Estratégico da Tecnologia da Informação e Plano Diretor de Tecnologia da Informação do Tribunal de Contas do Estado do Rio Grande do Norte é o documento que ainda serve de norte ao Órgão para a efetivação das ações na área de Tecnologia da Informação nele contempladas, apesar de não mais abrangido pelo período de vigência, e que, devido as exigências da LGPD, no decorrer do ano de 2020, o setor de Tecnologia da Informãtica propõe-se a elaborar um novo Planejamento para nortear as ações a serem desenvolvidas.

3.2 O TCE/PB x Proteção de Dados Pessoais

A Constituição do Estado da Paraíba, ao dispor sobre a organização do Poder Legislativo, no Capítulo I do Título V, dedicou a seção VIII à Fiscalização Contábil, Financeira, Orçamentária, Operacional e Patrimonial do Estado e das entidades da administração direta e indireta, a qual está distribuída do Art. 70 ao Art. 77. No artigo 71, enquadra o Tribunal de Contas como órgão auxiliar do Poder Legislativo no exercício do controle externo das entidades retromencionadas, ao passo que, do Art. 73 ao Art. 75, disciplina a sua estrutura e organização.

É da redação do Art. 74[172] e respectivo parágrafo único que se extrai a competência para que o próprio Tribunal de Contas regulamente as suas atribuíções definidas na Constituição Estadual. A lei de

[172] Art. 74. É da competência exclusiva do Tribunal de Contas elaborar o seu regimento interno, dispor sobre sua organização e funcionamento, eleger seus órgãos diretores e organizar sua secretaria e serviços auxiliares.
Parágrafo único. Lei de iniciativa do Tribunal de Contas estabelecerá sobre a sua organização, podendo constituir câmaras e delegações ou órgãos destinados a auxiliá-lo no exercício de suas funções, dispor sobre o seu quadro de pessoal, criação, transformação e extinção de cargos, fixação e alteração da respectiva remuneração.

inciativa do TCE/PB que estabelece sua organização é a Lei Orgânica - Lei Complementar Estadual nº. 18/93[173], 13 de julho de 1993, cujo detalhamento do funcionamento, eleição de órgãos diretores e organização de suas secretarias, em nível interno, está em seu Regimento Interno, qual seja, a RN-TC 010/2010 (com as alterações definidas até a RN-TC 02/2019). A estruturação e atribuições de seus cargos, ocupados por servidores públicos, concursados ou não, são disciplinadas pela Lei nº. 8.290, de 11 de julho de 2007, a qual dispõe sobre o Plano de Cargos, Carreiras e Remunerações dos Servidores do TCE/PB. Portanto, duas são as formas de regramento da organização e funcionamento do TCE/PB: mediante ato legal, sua lei orgânica e o palno de cargos e salários; e um ato normativo infralegal, o regimento interno.

Numa análise detalhada dos dois diplomas normativos, verifica-se que o TCE/PB dispõe de forma genérica ao tratar da área de informática, ou de tecnologia da informação. A teor da Lei Orgânica, prescreve o art. 63, *verbatim: "o Tribunal de Contas do Estado disporá de serviços para atender às atividades de apoio técnico e administrativo necessárias ao exercício de sua competência".*

As atividades desenvolvidas pela área de tecnologia da informação - TI estão inseridas nos serviços para atender às atividades de apoio técnico e administrativo, seja relativo à área meio seja no suporte ao controle externo, área fim. No mesmo sentido dispõe a lei de planos, cargos e salários, na denominação da área de TI e respectivas atribuições, explícitado na nota 3[174] ao estabelecer os requisitos do Assessor Técnico Chefe.

A nota 03 traz a denominação do cargo cujo nomeado incumbe-se da abrangente tarefa de supervisionar, técnica e administrativamente, a ASTEC, nome que qualifica o setor responsável pela área de tecnologia da informação do órgão. A seu turno, o Regimento Interno, ao dispor sobre a organização e composição do Tribunal de Contas, notadamente no Art. 5°, do Capítulo I, do Título II, insere a área de informática entre os órgãos internos de assessoramento técnico e administrativo[175].

---

[173] Cfe. texto integral da Lei Orgânica do TCE/PB. Disponível em: <https://tce.pb.gov.br/legislacao> . Acessado em: 28 de fev. 2020.

[174] Cfe. Lei nº. 8.290, de 11 de julho de 2007, que dispõe sobre o Plano de Cargos, Carreiras e Remunerações dos Servidores do Tribunal de Contas do Estado da Paraíba, e que estabelece os principais requisistos e atribuições de todos os cargos técnicos, a exemplo da Nota 03: ASSESSOR TÉCNICO CHEFE

Requisitos de Provimento: livre indicação do Presidente do Tribunal. Atribuições: Supervisionar, técnica e administrativamente, a Assessoria Técnica do Tribunal. Participar do planejamento técnico, administrativo e financeiro do Tribunal. Prestar assistência e apoio ao Presidente e aos membros do Tribunal no exame de problemas operacionais, administrativos e financeiros do Tribunal. Participar de outras tarefas de apoio técnico que lhe sejam conferidas pelo Presidente ou pelos membros do Tribunal. Disponível em: <https://tce.pb.gov.br/legislacao> . Acessado em: 28 de fev. 2020.

[175] Art. 5°. O Tribunal de Contas tem a seguinte composição:

I – Tribunal Pleno;

[...]

IX – Órgãos de Assessoramento Técnico e Administrativo;

O referido órgão de assessoramento técnico, a ASTEC, está em permanente trabalho visando normatizar suas atribuíções, tarefa esta que se mescla ao atendimento das demandas internas e ao desenvolvimento de ferramentas para dar suporte as auditorias realizadas pelo TCE-PB no exercício do controle externo.

Conciliar estas atribuições e adequá-las aos requisitos e princípios exigidos pela lei geral de proteção de dados pessoais é um desafio a ser enfrentado pela área de informática, não apenas no aspecto técnico propriamente dito, mas também no disciplinamento das responsabilidades a serem assumidas pelo material humano, seja este funcionários ou terceirizados, observadas as disposições legais de contratação de pessoal para terceirização dos serviços de informática.

Do conteúdo normativo disponível e acessível ao público, conforme os ditames da lei de acesso à informação, verifica-se que "meio eletrônico" é o termo recorrente que a Lei Orgânica do TCE/PB emprega ao referir-se ao uso de meios tecnólogicos no desempenho de suas atribuições e demais serviços, e que tal expressão ganhou força internamente a partir da publicação da Lei Complementar nº. 91, de 29 de outubro de 2009. Esta lei alterou a redação original da Lei Orgânica do TCE/PB, ao introduzir ao Título II o Capítulo V, composto de duas seções as quais instituíram, respectivamente, o Diário Oficial Eletrónico e o Processo Eletrónico no âmbito do TCE/PB.

O art. 59-A da Lei Orgânica esclarece objetivamente a que se presta o DOE/TCE, nos exatos termos: "Fica instituído o Diário Oficial Eletrônico do Tribunal de Contas do Estado - DOE/TCE como meio oficial de publicação dos atos processuais e administrativos do Tribunal e de seus órgãos integrantes, bem como das suas comunicações em geral". Com a instituição do DOE/TCE, a Lei Complementar nº. 91, de 29 de outubro de 2009, fez constar expressamente, no art. 59-B e no § 1° do mesmo artigo duas importantes regras que, em si, deram os primeiros indicativos legais da preocupação do órgão com a questão da proteção de dados, senão vejamos. Nos termos do art. 59-B, o *"Diário Oficial Eletrônico do Tribunal de Contas do Estado será disponibilizado na rede mundial de computadores – Internet, no sítio eletrônico do Tribunal de Conta"; por sua vez o § 1º. Estabelece que "as edições do Diário definido no caput serão assinadas digitalmente, atendendo aos requisitos de autenticidade, de integridade, de segurança e de validade jurídica na forma do Regimento Interno".*

Com efeito, a assinatura digital certificada, os requisitos de autenticidade e de integridade, que resguardam e confirmam a autoridade habilitada a produzir o ato formal, bem como a segurança e validade jurídica garantem a veracidade do conteúdo das edições do Diário Oficial Eletrónico a ser

---

X – Escola de Contas Conselheiro Otacílio Silva da Silveira;

XI – Ministério Público junto ao Tribunal. Disponível em: <https://tce.pb.gov.br/legislacao> . Acessado em: 28 de fev. 2020.

disponibilizado e acessível a todos na rede mundial de computadores. Ao Tribunal de Contas, contudo, são reservados os direitos autorais e de publicação DOE/TCE, ficando autorizada sua impressão, vedada, todavia, a comercialização, a teor do art. 59-D, da Lei Complementar nº. 91/ 2009. Este, sem equívoco, é o indicativo que mais se aproxima de uma noção interna de proteção de dados, o que longe está de espelhar o que dispõe a LGPD.

Outro importante passo com vistas a incrementar no âmbito interno e externo os avanços tecnológicos promovidos pela tecnologia da informação foi a instituição do sistema eletrónico de processos. A seção II da Lei Complementar nº. 91/2009 disciplinou os principais dispositivos sobre a matéria, o que contribuiu substancialmente para uma mudança de cultura dos agentes participantes do processo, tanto os funcionários quanto os jurisdicionados fiscalizados pelo TCE-PB, mediante contínuas ações de treinamento promovidos pelos técnicos de informática. Esta mudança de cultura representou um novo paradigma na forma de tratar os documentos, informações e dados a serem tramitados para e pelo Tribunal de Contas.

Neste norte, o Art. 59-E. da LCE nº. 91/ 2009 explicitou com clareza este novo paradigma ao instituir "[...] *no âmbito do Tribunal de Contas do Estado, o sistema eletrônico de processos por meio de autos, total ou parcialmente, digitais, utilizando, preferencialmente, a rede mundial de computadores e acesso por meio de redes internas e externas*". Passaram os atos processuais a serem realizados mediante o uso de sistemas eletrônicos de processos; os jurisdicionados passaram a enviar e receber dados e documentos que o TCE/PB repute necessários ao exercício da atividade de Controle Externo, na forma eletrônica, definidos em Regimento Interno, provimento específico ou decisão.

Paralelalmente à instituição do processo eletrónico, a lei que o criou também esboçou relativa preocupação com a proteção dos dados a serem tramitados eletronicamente. Segundo o Art. 59-G, *"a validade jurídica dos dados, documentos e os atos processuais na forma digital condiciona-se à assinatura eletrônica";* e segue com o parágrafo único, ao estabelecer que serão considerados originais para todos os efeitos legais os documentos produzidos eletronicamente e juntados aos processos eletrônicos, bem como os dados eletrônicos armazenados nos bancos de dados do Tribunal, desde que com garantia de sua origem e de seu signatário.

Convém salientar que, com a iminente entrada em vigor da LGPD, programada para meados de 2020, os Tribunais de Contas do Brasil mobilizam-se no sentido de padronizar os procedimentos internos com objetivo de facilitar a adequação de suas normas àquele diploma normativo**.** Neste sentido, o TCE/PB tem desenvolvido ferramentas internas por meio da ASTEC, aparelhando e treinando seus servidores/funcionários, ao tempo em que, em relação aos seus jurisdiconados, fez constar na própria Lei Complementar nº. 91/2009 que a mudança de procedimentos do suporte em meio físico para o eletrônico

obriga-os ao uso do meio eletrônico, salvo disposição expressa em contrário no Regimento Interno ou norma específica[176].

É um desafio o cumprimento desde desidério, considerando toda a logística envolvida, os custos de material tecnológico e os recursos disponíveis para fazer frente a tais investimentos.

3.3 O Tribunal de Contas de Portugal x Proteção de Dados Pessoais

O Tribunal de Contas de Portugal, diferentemente dos retrocidados Tribunais de Contas do Brasil, apresenta a disciplina normativa acerca dos serviços de apoio técnico e administrativo por meio do Decreto-Lei n.º 440/99, de 2 de novembro de 1999, oficialmente conhecido sob a denominação de Estatuto dos Serviços de Apoio do Tribunal de Contas (ESATC). E o faz, a organização e funcionamento, de forma precisa e didática sobre a qual dedicar-se-á este tópico do trabalho.

Ao abrigo do disposto no n.º 6 do artigo 5.º, do Decreto-Lei n.º 440/99, de 2 de novembro, o instrumento normativo interno que disciplina sobre o DSTI, cuja iniciativa é de competência do Diretor-Geral do Tribunal de Contas, observadas as linhas gerais de organização e funcionamento aprovadas pela Resolução n.º 1/00-CP, é o Despacho n.º 46/2000-GP, de 27 de abril, com as alterações introduzidas pelos Despachos n° 140/2000-GP, de 20 de dezembro; 10/2001-GP, de 6 de fevereiro; 71/2003-GP, de 18 de dezembro; 11/2005-GP, de 9 de março; e 47/2010-GP, de 29 de dezembro[177].

O n° 1 do Artigo 1.º do Capítulo I do Despacho n.º46/2000-GP delinea a estrutura da Direção-Geral do Tribunal de Contas (DGTC), a qual subdivide-se em dois departamentos, quais sejam, o de apoio técnico-operativos (DAT) e o de apoio instrumental (DAI), sendo sob a égide deste último que se encontra o Departamento de Sistemas e Tecnologias de Informação (DSTI). Além deste Departamento, cujas atividades são de amplo espectro dentro do Tribunal de Contas, o n° 4 do mesmo Artigo 1.° traz em seu conteúdo a criação do Núcleo de Apoio Técnico ao Desenvolvimento de Auditorias dos Sistemas Informáticos e em Ambiente Informático (NATDA), diretamente dependente da Direção-Geral, cujo cargo é ocupado por um Juiz-Conselheiro.

Como se pode aferir, o Tribunal de Contas de Portugal alçou a sua área de Tecnologia da Informação a uma posição de destaque em sua organização e estrutura, tamanha a importância das

---

[176] Cfe. § 2° do Art. 104-E, precedido pelo § 1° o qual assim dispõe: "*O Tribunal de Contas poderá implantar os procedimentos citados no caput deste artigo de forma gradativa, respeitando o planejamento de informatização adotado*". Disponível em: <http://portal-antigo.tce.pb.gov.br/wp-content/uploads/2018/05/2-9380_texto_integral.pdf>. Acessado em: 28 de fev. de 2020.

[177] Cfe. Coletânea de Legislação do Tribunal de Contas na parte relativa às publicações de livre acesso. Disponível em: <https://www.tcontas.pt/pt-pt/TribunalContas/Publicacoes/ColetaneasLegislacao/Documents/legis2020.pdf>. . p. 149-172. Acessado em: 02 de mar. de 2020.

atividades a serem aí desenvolvidas, o que, de certa forma, tem tornado mais fácil a adequação aos requisitos exigidos pelo RGPD.

O Art. 8° do Capítulo I define e estabelece as principais atribuições do DSTI, e cumpre-nos fazer uma breve análise da atividade por ele desempenhada e o nível de vinculação com o que dispõe o RGPD, à luz dos estudos internos realizados pelos Técnicos do Tribunal de Contas com vistas à aplicação das regras de proteção de dados na Instituição. Neste norte, assim explicita o n° 1 do Art. 8° do Despacho n.º46/2000-GP: *"o DSTI é o departamento de apoio instrumental que tem por missão a concepção e permanente adaptação dum sistema integrado de gestão e informação para utilização do Tribunal e dos Serviços de Apoio, compreendendo, nomeadamente, subsistemas de gestão de entidades e de gestão processual, incumbindo-lhe, designadamente [...]".*

A missão do DSTI, qual seja a concepção e permanente adaptação dum sistema integrado de gestão e informação, alinha-se ao novo modelo do planejamento estratégico aprovado pelo Plenário Geral em 20 de março de 2019, com vigência trienal (2020-2022), por meio do qual foram identificados os principais eixos que caracterizam o contexto interno e externo do Tribunal de Contas de Portugal, tendo em vista identificar os fatores principais que influenciam as suas atividades bem como o seu desempenho ante a sociedade[178].

Em sua mensagem de apresentação ao Planeamento Estratégico, o Presidente do Tribunal de Contas, Juiz Conselheiro Vitor Caldeira, fez questão de enfatizar no referido documento, entre os quatro objetivos estratégico a que se propôs realizar, a "*preocupação sistemática com a flexibilidade, encarada como capacidade de ajustamento às mudanças rápidas e imprevistas próprias de uma realidade globalizada, interligada e digitalizada*", o que requer "*um significativo investimento na modernização e reorganização da sua estrutura e modus operandi, bem como na qualificação e rejuvenescimento dos seus recursos humanos*. E acrescenta, ainda, que *"[...] para a sua concretização são identificados vários eixos prioritários de ação, que visam responder aos riscos e desafios identificados, nomeadamente os relativos à preparação para a sociedade digital, ao desenvolvimento sustentável*"[179].

Entre os eixos prioritários de ação, com vistas à automatização de procedimentos de rotina, o DSTI deverá envidar esforços e estudos para promover a segurança da informação, a habilitação em meios e competências digitais, a desmaterialização e automação de processos e procedimentos, com recurso à inteligência artificial, na fiscalização prévia, nas várias formas de fiscalização concomitante e sucessiva e nos julgamentos, bem como no controlo dos dados e informações em nível interno.

---

[178] Cfe. Plano Estratégico estabelecido para o triênio 2020/2022. Material de livre acesso. Disponível em: <https://www.tcontas.pt/pt-pt/Transparencia/PlaneamentoGestao/PlanosTrienais/Documents/plano_estrategico_vf_internet_hp_20191106.pdf>. Acessado em 02 de mar. 2020.

[179] Ibid.

Antes mesmo deste norteamento oficializado pelo Planeamento Estratégico, o Tribunal de Contas dedicara-se ao estudo[180] e à edição normativa interna, tendo em vista a entrada em vigor do RGPD. Destarte, como consequência deste estudo, o Plenário Geral aprovou e fez publicar a Resolução n° 3/2018-PG cujo objeto é a aplicação do RGPD no Tribunal de Contas e seus Serviços de Apoio.

Com a referida Resolução foram implementadas duas medidas fundamentais ao processo de adequação de suas normas ao RGPD, quais sejam: a) a adequação da publicitação do conteúdo dos atos do Tribunal ao princípio da minimização de dados; e b) a designação de um Encarregado de Proteção de Dados e a definição de seu estatuto. Paralelamente a tal iniciativa, a Assembleia da República apreciara a Proposta de Lei n° 126/XIII[181], cujo objeto é a adpatação de algumas disposições do RGPD ao sistema judicial, no qual o Tribunal de Contas se insere, e a qual deverá se valer notadamente em relação à atribuição de poderes aos juízes e relatores de processos e atos jurisdicionais ou de controlo financeiro, enquanto responsáveis pelo tratamento e proteção de dados no âmbito daqueles atos e processos, em articulação com a ação a desenvolver pelo Encarregado de Proteção de Dados, nos termos previstos na RGPD.

A Resolução faz referência ao Regulamento Geral do Tribunal de Contas[182], notadamente ao Art. 13°, segundo o qual "*o Tribunal de Contas define uma estratégia de comunicação, adequada ao cumprimento do seu mandato, com a observância dos princípios da transparência, da prestação de contas e da proteção de dados pessoais, designadamente através da divulgação dos resultados em tempo oportuno";* bem como à alínea c), n° 2 do Art. 19°, por meio do qual se estabelece uma competência específica à Comissão de Informática, a de *"assegurar o cumprimento dos dispositivos legais, designadamente relativos à proteção de dados pessoais"*.

Atendendo ao que dispõe o retrocitado Art. 13° do Regulamento do Tribunal de Contas, a adequação da publicitação do conteúdo dos atos do Tribunal ao princípio da minimização dos dados visa a garantia de que os atos publicados pelo Tribunal não contém informações pessoais que vão além do necessário e que atende ao interesse público a que se presta a respetiva publicação, o que está em

[180] A aplicação no Tribunal de Contas e Serviços de Apoio do RGPD foi objeto de estudos preparatórios consubstanciados no Estudo n° 2/2018-DCP e na Informação n° 17/2018-DCP. Conforme explicitado na Resolução n° 3/2018-PG. Disponível em: <https://www.tcontas.pt/pt-pt/NormasOrientacoes/Resolucoes/Documents/2018/res003-2018-pg.pdf>. Acessado em 02 de mar. 2020.

[181] Através da presente proposta de lei, pretende-se alterar pela segunda vez a Lei n.º 34/2009, de 14 de julho, que estabelece o regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial, adaptando-a ao disposto no Regulamento (UE) n.º 2016/679, do Parlamento e do Conselho, de 27 de abril de 2016 ("o Regulamento"), e na Lei n.º [PL 120/XIII] que assegura a sua execução na ordem jurídica interna, assim como o disposto na Lei n.º [Reg.º PL 74/2018], que transpõe para a ordem jurídica interna a Diretiva (UE) n.º 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 ("a Diretiva"). Exposição de motivos. Disponível em: <www.parlamento.pt/actividadeparlamentar> . Acessado em: 28 de dez. de 2019.

[182] Regulamento 112/2018, aprovado pelo Plenário Geral, em reunião de 24 de janeiro de 2018. Disponível em: <www.tcontas.pt/publicações>. Acessado em: 28 de dez. de 2019.

sintonia com as alíneas b) e c) do número 1 do Art. 5° do RGPD. Alguns procedimentos, não exaustivos, deverão ser observados pelo Tribunal de Contas com o objetivo de estar em linha com o princípio da minimização, a teor da citada Resolução, senão vejamos, em síntese:

- A fim de se resguardar o interesse público buscado sem prejuízo da observância do direito à proteção de dados pessoais, são consideradas legítima, adequada, necessária e proporcional, a explicitação, na publicação dos atos do Tribunal citados no parágrafo acima, do nome e cargo das pessoas em causa desde que sujeitos à jurisdição do próprio Tribunal. Neste caso, devem ser omitidos outros dados pessoais, exceto se restar demonstrado que tais dados têm relevância pública;

- No tocante à publicação de acórdãos, sentenças, relatórios de auditoria e outros atos do Tribunal, bem como os atos do Ministério Público que com àqueles guardam conexão, o conteúdo deve restringir-se apenas aos dados pessoais indispensáveis à informação da sociedade acerca da utilização dos recursos públicos e à garantia da *accountability*[183] dos gestores e respectivos responsáveis desses recursos.

- Deverá ser ponderada a eventual desnecessidade de se fazer referências na publicitação dos atos a empresas ou putros sujeitos privados, si;ngulares ou coletivos, de relações jurídicas com entidades públicas sujeitas à jurisdição do Tribunal e que não tyenham qualquer responsabilidade pela gestão ou pela utilização de dinheitos ou ativos públicos;

- O Juiz Conselheiro Relator é o responsável por identificar os dados pessoais que devam ser omitidos, entretanto, sempre que houver dúvidas sobre os dados pessoais que podem constar na publicação dos mencionados atos do Tribunal de Contas, o Encarregado de Proteção de Dados do Tribunal deverá ser consultado;

Estes são os principais procedimentos a serem observados e realizados pela área de Tecnologia da Informação com vistas à escorreita adequação da publicitação do conteúdo dos atos do Tribunal de Contas. Vejamos, nas linhas seguintes, o que a Resolução estabelece quanto à figura do Encarregado de Proteção de Dados e o que prescreve em relação ao seu estatuto.

---

[183] Este princípio é o da responsabilização das pessoas encarregadas de um tratamento de dados pessoais. Por exemplo, cada empresa ou Entidade Pública deve avaliar a sua política e a gestão dos riscos envolvidos para preparar as respostas adequadas. O que fazer em caso de ataques cibernéticos, de roubos de dados ou de hacking? Como é que os seus dados passam pelos seus serviços e quem pode ter acesso a eles? O que faz para os proteger, respeitando a confidencialidade e certificando-se de que os pedidos de supressão ou de alteração estão bem implementados? Este trabalho de responsabilização comum e global exige o envolvimento de todas as partes interessadas da empresa ou Entidade Pública, que devem ser coordenadas por um piloto, responsável pela missão ou representante na pessoa de um Encarregado de Proteção de Dados (geralmente chamado "DPO" para *Data Privacy Officer).* Parte da doutrina aponta a *accountability, a Privacy by design* e responsabilidade conjunta entre responsáveis de tratamento e subcontratantes como os três grandes princípios do RGPD, que fazem parte das novas obrigações, transformando a forma de gerir os dados. Disponível em: https://blog.kwanko.com/pt-pt/dados-pessoais-rgpd-esta-pronto/ . Acessado em: 28 de dez. de 2019.

Salienta Ana Fazendeiro[184] "[...] *que a figura do encarregado de proteção de dados não existia na Diretiva 95/46/CE, embora já fosse prevista nas legislações de diversos países da comunidade europeia, com especial destaque para a lei alemã, a qual serviu de inspiração para o RGPD"*. Segundo a autora retrocitada, *"[...] a Bundesdatenschutzgesetz (BDSG), isto é, a Lei Federal Alemã de Proteção de Dados impõe às entidades nas quais haja no mínimo 9 trabalhadores que exerçam suas atividades exclusivamente no tratamento automatizado de dados ou, alternativamente, nas quais pelo menos 20 trabalhadores realizem tratamento não automatizado de dados, que nomeiem um encarregado de proteção de dados. Para atender as exigências da lei tedesca, a pessoa nomeada para tal função (em geral, um profissional ou empresa contratados em regime de outsourcing[185]) deve ser um profissional altamente qualificado, o qual goza da proteção em situação de despedimento, salvo na hipótese de descumprimento grave de seus deveres legais"*.

Nesta esteira, o art. 37° do RGPD, ao dispor sobre a designação do EPD[186] obriga algumas

---

[184] FAZENDEIRO, Ana. Regulamento Geral sobre a Proteção de Dados. - 3ª ed. – (textos da lei). Coimbra. ALMEDINA. Setembro, 2018. P. 19.

[185] *Outsourcing* é a prática de terceirizar serviços ligados à parte estratégica da empresa, ou seja, buscar fontes externas para fazer estes trabalhos. Disponível em: <https://www.significados.com.br/outsourcing/>. Acessado em: 23 de dez. de 2019.

[186] ARTIGO 37°

Designação do encarregado da proteção de dados

1. O responsável pelo tratamento e o subcontratante designam um encarregado da proteção de dados sempre que:

   a) O tratamento for efetuado por uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional;(grifo nosso)

   b) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou

   c) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados nos termos do artigo 9° e de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10°.

2. [...]
3. Quando o responsável pelo tratamento ou o subcontratante for uma autoridade ou um organismo público, pode ser designado um único encarregado da proteção de dados para várias dessas autoridades ou organismos, tendo em conta a respetiva estrutura organizacional e dimensão.
4. [...]
5. O encarregado da proteção de dados é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções referidas no artigo 39.°.
6. O encarregado da proteção de dados pode ser um elemento do pessoal da entidade responsável pelo tratamento ou do subcontratante, ou exercer as suas funções com base num contrato de prestação de serviços. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32016R0679>. Acessado em: 30 de jan. 2020.

Instituições (Pessoas coletivas ou Entidades Públicas) a nomearem um encarregado de proteção de dados, tendo em conta as suas qualidades profissionais e, em especial, os seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções especificadas no Regulamento.

Interessa-nos, em princípio, a ressaltada aliena a), a qual se refere à autoridade ou organismo público. Com efeito, à luz do disposto no aludido Art. 37°, o item 2 e respectivos subitens da Resolução n° 3/2018-PG delibera acerca da nomeação e estatuto, bem como da missão e funções do Ecarregado de Proteção de Dados no âmbito do Tribunal de Contas.

De pronto, a Resolução reconhece o dever do Tribunal de Contas de nomear um EPD, e o fez na pessoa do Presidente da Comissão de Informática, conforme expresso no item 3[187] da norma interna. Para designação do seu EPD, o TC. de Portugal fez-se valer dos requisitos do n° 5 e do n° 6 do Art. 37° do RGPD, supra evidenciados, levando em conta os conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como na capacidade do designado para desempenhar as funções referidas no artigo 39.° do RGPD[188], além de outras que lhe possam ser atribuídas.

A par disso, a Resolução confere ao EPD a missão de promover a adoção e de zelar pela aplicação das medidas técnicas e organizativas, no âmbito do Tribunal de Contas e seus Serviços de Apoio, para assegurar e poder comprovar que o tratamento de dados pessoais é realizado em conformidade com o RGPD.

---

[187] Para efeitos do disposto dos artigos 37°, 38° e 39° do RGPD, no Tribunal de Contas e seus Serviços de Apoio o Encarregado de Proteção de Dados é o Presidente da Comissão de Informátiuca, cujo titular neste momento é a Senhora Conselheira Helena Abreu Lopes. Conforme explicitado na Resolução n° 3/2018-PG. Disponível em: <https://www.tcontas.pt/pt-pt/NormasOrientacoes/Resolucoes/Documents/2018/res003-2018-pg.pdf>. Acessado em 02 de mar. 2020.

[188] Artigo 39°

Funções do encarregado da proteção de dados

1. O encarregado da proteção de dados tem, pelo menos, as seguintes funções:

a) Informa e aconselha o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União ou dos Estados-Membros;

b) Controla a conformidade com o presente regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;

c) Presta aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos do artigo 35°;

d) Coopera com a autoridade de controlo;

e) Ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36.°, e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto.

2. No desempenho das suas funções, o encarregado da proteção de dados tem em devida consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento. Disponível em:< https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32016R0679>. Acessado em: 30 de jan. 2020.

Para dirimir aparente conflito em relação a pessoa do Encarregado que se presta a atender as Secções Regionais do Tribunal de Contas em Madeira e nos Açores, a Resolução encontrou guarida no n° 3 do artigo 37° do RGPD o qual autoriza a designação de "*...um único encarregado da proteção de dados para várias dessas autoridades ou organismos, tendo em conta a respetiva estrutura organizacional e dimensão",* o que se aplica para a Sede do TC em Lisboa e para as Secções da Madeira e dos Açores.

No tocante à posição do EPD, conforme os ditames do Art. 38° do RGPD[189], a Resolução n° 3/2018-PG foi precisa e direta. Assim, estabeleceu que ao dito Encarregado deve ser assegurado o envolvimento em todas as questões relacionadas com a proteção de dados pessoais, de forma adequada e em tempo útil, nos termos do n.° 1 do Art. 38° do RGPD; ademais, devem ser-lhe facultados os recursos necessários ao desempenho de suas funções e à manutenção de seus conhecimentos, devendo ser-lhe dado acesso aos dados pessoais e às operações de tratamento, conforme o n.° 2 do art. 38° do RGPD.

Em relação às exigências do n.° 3 do art. 38° do RGPD, o Encarregado de Proteção de EPD reporta-se ao Plenário Geral do Tribunal. Em atenção aos n.°s 4 e 5 do mesmo artigo, a Resolução deixa assegurado que os titulares dos dados podem contactar o EPD sobre todas as questões relacionadas com o tratamento de seus dados pessoais e com o excercício dos direitos que lhe são conferidos pelo RGPD, ao tempo em que vincula o EPD à obrigação de sigilo ou de confidencialidade no exercício das funções que lhes forem atribuídas em consonância com o art. 39°, e em conformidade com o direito da União ou dos Estados-Membros.

Com espectro no n.° 6 do art. 38°, a Resolução confere ao EPD a possibilidade de exercer

[189] Artigo 38°

Posição do encarregado da proteção de dados

1. O responsável pelo tratamento e o subcontratante asseguram que o encarregado daproteção de dados seja envolvido, de forma adequada e em tempo útil, a todas as questões relacionadas com a proteção de dados pessoais.
2. O responsável pelo tratamento e o subcontratante apoia o encarregado da proteção de dados no exercício das funções a que se refere o artigo 39.°, fornecendo-lhe os recursos necessários ao desempenho dessas funções e à manutenção dos seus conhecimentos, bem como dando-lhe acesso aos dados pessoais e às operações de tratamento.
3. O responsável pelo tratamento e o subcontratante asseguram que da proteção de dados não recebe instruções relativamente ao exercício das suas funções. O encarregado não pode ser destituído nem penalizado pelo responsável pelo tratamento ou pelo subcontratante pelo facto de exercer as suas funções. O encarregado da proteção de dados informa diretamente a direção ao mais alto nível do responsável pelo tratamento ou do subcontratante
4. Os titulares dos dados podem contactar o encarregado da proteção de dados sobre todas questões relacionadas com o tratamento dos seus dados pessoais e com o exercício dos direitos que lhe são conferidos pelo presente regulamento.
5. O encarregado da proteção de dados está vinculado à obrigação de sigilo ou de confidencialidade no exercício das suas funções, em conformidade com o direito da União ou dos Estados-Membros.
6. O encarregado da proteção de dados pode exercer outras funções e atribuições. O responsável pelo tratamento ou o subcontratante assegura que essas funções e atribuições não resultam num conflito de interesses. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32016R0679>. Acessado em: 30 de jan. 2020.

outras funções e atribuições, sob a condição de que inexista conflito de interesses e tendo em mente os riscos associados às operações de tratamento, de acordo com a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados. Desta forma, levando em conta a especificidade da atividade desenvolvida pelo Tribunal de Contas e seus Serviços de Apoio, ao EPD foram-lhe atribuídas as seguintes funções, as quais, para efeitos didáticos podem ser denominadas: de consultoria (aconselhamento); de garantidor de segurança dos dados; avaliador da segurança dos dados; de executor de procedimentos e ações de melhoria.

No desempenho da função de consultoria, cabe ao EPD aconselhar, em caso de dúvida, sobre a admissibilidade da publicação de determinados dados pessoais constantes de relatórios de auditoria, sentenças, acórdãos e despachos, bem como Aconselhar sobre a informação a prestar aos titulares de dados fornecidos para fins específicos, e sobre a aprovação e atualização; e pronunciar-se, se solicitado, sobre a regulamentação (ou projeto de regulamentação) do Sistema de Informação a que se refere o artigo 18° do Regulamento do Tribunal de Contas[190].

Atuando como garantidor da segurança de dados, compete ao EPD promover a adoção de procedimentos internos de garantia do exercício dos direitos dos titulares dos dados, designadamente no que diz respeito à tramitação dos pedidos feitos por eles.

Como avaliador, deve o EPD promover a avaliação do nível de segurança dos dados conservados pela DGTC, designadamente os referentes aos dados pessoais de juízes conselheiros e pessoal dos Serviços de Apoio; identificar os dados que devam ser classificados como "dados sensíveis" e avaliar e propor o ajustamento, quando necessário, do respectivo nível de segurança; e avaliar o nível de segurança e dos procedimentos de gestão e acesso às bases de dados dos Serviços de Apoio, incluindo a base GENT, propondo as alterações que considere necessárias.

Ao atuar como executor de procedimentos e ações de melhoria, o EPD poderá propor a inclusão no plano de formação dos Serviços de Apoio de ações de formação relacionadas com a temática

---

[190] Artigo 18.º

Regulamentação

1. O sistema de informação é regulamentado pelo Presidente tendo em conta as orientações gerais definidas pelo Plenário Geral, e deverá contemplar:

a) A identificação do gestor ou responsável pelo sistema e definição das respetivas funções;

b) A definição de níveis de acesso à informação para efeitos de registo e consulta;

c) A definição de níveis de gestão da rede;

d) A criação de indicadores de alerta que identifiquem tentativas de intrusão e respetiva origem;

e) A definição de critérios gerais e níveis de competência relativos à disponibilização de informação para o exterior.

2. A regulamentação do sistema de informação deverá ainda respeitar as disposições legais e regulamentares relativas à proteção de dados pessoais. (Regulamento 112/2018, aprovado pelo Plenário Geral, em reunião de 24 de janeiro de 2018). Disponível em: <www.tcontas.pt/publicações>. p. 105. Acessado em: 28 de dez. de 2019

do tratamento e segurança de dados pessoais, bem como propor a adoção de medidas técnicas e de procedimento que considere necessárias ao cumprimento do RGPD, a minimização de riscos de segurança, os procedimentos a adotar em caso de quebras de segurança eidentificação dos respectivos responsáveis.

Por fim, a Resolução n° 3/2018-PG impõe ao EPD a obrigação de apresentar ao PG-TC, até o dia 30 de maio de cada ano, um relatório de suas atividades realizadas no ano anterior. Tal incumbência, não retira a relativa autonomia do EPD, apenas atribui-lhe um dever institucional de prestar contas de suas atividades, o que se traduz numa forma de exercício de controle interno, a exemplo dos demais setores do Tribunal de Contas.

Cumpre salientar que, após a publicação de supra referida Resolução, o TC. de Portugal tem se aprofundado no estudo da temática da proteção de dados pessoais, notadamente por meio de seus técnicos vinculados à Comissão de Informática[191] prevista no art. 19° do Regulamento 112/2018, de 15 de fevereiro.

Os estudos desenvolvidos pelos membros da Comissão de Informática estão precipuamente concentrados na problemática da adequação do RGPD ao Tribunal de Contas, tendo como norte o disposto no Considerando 20 daquele Regulamento, o qual determina expressamente que seja aplicado os seus requisitos às atividades dos tribunais e de outras autoridades judiciais. No percurso dessa paulatina adequação de normas, o Tribunal de Contas tem estado atento ao referido considerando 20, posto que este traz em seu conteúdo uma importante ressalva, ao excluir da competência das autoridades de controlo o tratamento de dados pessoais efetuado pelos Tribunais no exercício de sua função jurisdicional, assegurando, dessa forma, a independência do poder judicial no exercício de sua função jurisdicional, nomeadamente a tomada de decisões, evitando que uma autoridade administrativa interviesse no exercício daquela função.

Ainda no decorrer deste trabalho, far-se-á menção a alguns dos documentos produzidos pelo TC. de Portugal cujos conteúdos promovem a esperada adequação ao RGPD. Isto será objeto de apreciação no capítulo que se segue, posto que haverá a possibilidade de fazer-se um paralelo entre os Sistemas de Acompanhamento de Gestão dos TC's pesquisados e as disposições da LGPD, e do RGPD.

---

[191] Artigo 19.º

Comissão de Informática

O sistema de informação é acompanhado permanentemente por uma Comissão de Informática presidida por um Juiz Conselheiro eleito pelo Plenário Geral, por um magistrado do Ministério Público, pelo gestor ou responsável pelo sistema de informação e por um técnico dos Serviços de Apoio nomeado pelo Presidente. Disponível em: <www.tcontas.pt/publicações>. Acessado em: 28 de dez. de 2019

Capítulo IV – Sistemas de Gestão dos TCs e proteção de dados

Neste capítulo, pretende-se apresentar a realidade encontrada nos Tribunais de Contas objeto de análise do presente trabalho, notadamente no que diz respeito a relação entre os sistemas de acompanhamento de gestão de cada um deles e as ferramentas disponíveis para tornar viável a efetiva e adequada proteção de dados pessoais cooptados por estas Entidades Públicas ao realizar as funções constitucionais no exercício de suas competências.

É cediço que um sistema de acompanhamento de gestão desenvolvido pela área de Tecnologia da Informação de cada um dos TC's que ora se estuda não se restringe à proteção de dados pessoais, sendo-lhe exigido buscar as ferramentas que visem facilitar e dar suporte a todas as atividades contempladas em seus respectivos regulamentos internos, sejam relacionadas à área-meio, sejam afetas à área-fim. Contudo, em quaisquer delas são manipulados dados e, a estes, se prestam os requisitos a serem observados para a devida proteção.

Como poderemos constatar, os três Tribunais de Contas dispõem de sistemas distintos de gestão, quais sejam: o Sistema Integrado de Auditoria Informatizada (SIAI Fiscal), no TCE/RN; o Sistema de Acompanhamento da Gestão dos Recursos da Sociedade (SAGRES), no TCE/PB; e o sistema de gestão de entidades (GENT), no Tribunal de Contas de Portugal. Tais sistemas, porém, convergem no que diz respeito ao zelo pelo tratamento de dados e informações que lhes são alimentadas pelos jurisdicionados e demais entidades objeto da ação fiscalizadora desenvolvida no âmbito de suas competências.

Os sistemas de acompanhamento de gestão desenvolvido pela área de TI de cada um dos TC's consistem em um software inteligente cujo objetivo é a facilitação das atividades desenvolvidas pelos seus diversos setores, automatizando o máximo de processos possível.

O desafio a ser enfrentado, ante os requisitos exigidos pelas legislações de proteção de dados (RGPD e LGPD), requer dos funcionários do setor de TI uma revisão detalhada do sistema já em operação para, num segundo momento, adequar as ferramentas disponíveis as regras de proteção de dados dos titulares envolvidos que, no caso dos TC's, não se limitam apenas aos ocupantes de cargos em sua estrutura interna, senão também e, principalmente, aos dados alimentados pelos titulares das diversas esferas de poder (Estados e Municípios).

Passemos, então, à análise dos principais aspectos levantados quando da visita e estudo dos respectivos Sistemas de Tecnologia da Informação de cada Tribunal de Contas e o suporte ao acompanhamento da gestão que tais ferramentas ofertam, levando em conta os princípios aplicáveis ao tratamento de dados e os direitos dos titulares destes dados, conforme os ditames das legislações de

proteção de dados (RGPD e LGPD), sem olvidar dos já conhecidos benefícios resultado de um eficiente sistema de gestão, tais como: maior sustentabilidade na utilização dos recursos dos TCs; maior segurança para os funcionários; melhoria nos índices de satisfação interna.

4.1. TCE/RN – SIAI

O SIAI Fiscal, normatizado pela Resolução TCE N° 11/2016[192], de 9 de junho de 2016, consiste em um programa informatizado desenvolvido pela Diretoria de Informática do TCE/RN, para possibilitar o acompanhamento e o controle sobre a execução orçamentária e financeira dos entes públicos sob sua jurisdição, com vistas à averiguação da regularidade da gestão pública.

Este objetivo do SIAI materializa-se no envio periódico de uma série de dados pelas prefeituras e órgãos governamentais para análise das contas pelo TCE/RN. Quando da preparação deste aplicativo, o TCE/RN disponibilizou aos seus jurisdicionados novos layouts e modelos de importação com o objetivo de padronizar o envio de dados e possibilitar a leitura pelo sistema.

Periodicamente, a Diretoria de Informática faz a atualização do sistema e disponibiliza as novas versões aos jurisdicionados, de tal forma que os dados sejam alimentados de acordo as exigências promovidas pelas alterações das legislações federais, estaduais e municipais. As modificações e incremento nas ferramentas de tecnologia da informação tem levado em conta as disposições normativas da LGPD, especificamente no que diz respeito à alimentação dos dados pelos fiscalizados do TCE/RN, dados estes que consistem em relatórios e demonstrativos exigidos por lei e por atos normativos do próprio Tribunal que visam dar transparência e publicidade à execução das políticas públicas e atos de gestão dos titulares de Poderes (Estado e Município).

A título de exemplificação, a atual versão (2020) do SIAI incorporou as alterações implementadas pela Resolução n° 018/2019-TCE, de 12 de dezembro de 2019, que limitou a obrigação de limitar a ferramenta apenas a chefes do Poder Executivo do Estado e dos Municípios (Governadores e Prefeitos) para fins de envio das informações do Relatório Resumido de Execução Orçamentária - RREO e a titulares dos Poderes e órgãos para fins de envio das informações do Relatório de Gestão Fiscal - RGF. Os retrocitados relatórios são exigidos pela Lei de Responsabilidade Fiscal[193], a qual

[192] Regulamenta os modos de organização, composição e elaboração de documentos, procedimentos e demonstrativos previstos na Lei de Responsabilidade Fiscal, bem como de processos de execução da despesa pública, no âmbito do Estado do Rio Grande do Norte e dos seus respectivos Municípios, estabelece formas e prazos para sua apresentação ao Tribunal de Contas e dá outras providências.. Disponível em: <http://www.tce.rn.gov.br/Legislacao/ResolucoesTce>. Acessado em: 12 de mar. de 2020.

[193] Lei n° 101/2000, de 4 de maio de 2000 - Estabelece normas de finanças públicas voltadas para a responsabilidade na gestão fiscal e dá outras providências. Aplicável a todos os Entes da Federação. Disponível em: < http://www.tce.rn.gov.br/Legislacao/LeisComplementaresFederais> .Acessado em: 18 de mar.2020.

estabelece, entre outras, que a responsabilidade na gestão fiscal pressupõe a ação planejada e transparente, em que se previnem riscos e corrigem desvios capazes de afetar o equilíbrio das contas públicas, o que exige dos órgãos de Controle Externo, a exemplo dos Tribunais de Contas, uma permanente atualização dos seus sistemas de informação, visando a garantia dos princípios constitucionais da legalidade e eficiência.

Em sua versão original, nos termos do §1º da Resolução n° 11/2016, o SIAI do TCE/RN compõe-se de dois subsistemas: a) o MÓDULO COLETA, voltado para a captação de documentos, dados e informações acerca da gestão no âmbito dos entes públicos jurisdicionados, por meio dos relatórios e demonstrativos previstos na LRF, adaptados dos modelos definidos nas Portarias da STN, além de outros criados pelo próprio Tribunal; e b) o MÓDULO RECEPÇÃO, MÓDULO ANÁLISE e MÓDULO DIVULGAÇÃO, viabilizadores do tratamento a ser dispensado pelo Tribunal aos documentos, dados e informações efetivamente coletados.

O SIAI, a despeito das exigências da LGPD, porém, embasado nos dispositivos da Lei n° 12.527, de 18 de novembro de 2011, a denominada lei de acesso à informação, subdivide-se nos dois subsistemas supra evidenciados, os quais observam procedimentos que se destinam a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública[194], previstos na Constituição da República Federativa do Brasil e com base em algumas diretrizes, entre as quais destacam-se a observância da publicidade como preceito geral e do sigilo como exceção, a divulgação de informações de interesse público, independentemente de solicitações e a utilização de meios de comunicação viabilizados pela tecnologia da informação.

Destarte, a Diretoria de Informática do TCE/RN, tendo em conta a existência da Lei de Acesso à Informação e a emergente Lei Geral de Proteção de Dados, vem envidando esforços no sentido de conciliar as disposições das duas legislações, de tal forma que os aludidos subsistemas preservem os direitos fundamentais dos titulares dos dados, mormente os de seus jurisdicionados, ou das pessoas que os representam. É um estudo dinâmico e permanente, pois requer o conhecimento prévio dos dois diplomas normativos, a conciliação dos seus dispositivos e o desenvolvimento de ferramentas de tecnologia de informação que atendam as demandas, sem conflitar interesses protegidos constitucionalmente.

Interessa-nos, pois, apresentar o estágio atual dos subsistemas do SIAI, de que forma eles se afiguram e interagem com os requisitos da LGPD, sabendo-se, contudo, que novas versões estão sendo

[194] Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte: [...]. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acessado em: 20 de mar. 2020.

desenvolvidas visando alcançar níveis adequados de proteção de dados, segundo as regras e princípios da referida lei de proteção de dados.

Neste norte, o MÓDULO COLETA, primeiro dos subsistemas do SIAI, compreende em sua formatação os seguintes itens: o Ambiente Desktop, denominado SIAI FISCAL COLETA DESKTOP, que é destinado à preparação e validação prévia dos dados referentes aos anexos que compõem o Relatório Resumido de Execução Orçamentária - RREO e o Relatório de Gestão Fiscal - RGF; o Ambiente Web, integrado ao Portal do Gestor[195], destinado para envio dos dados gerados a partir do SIAI FISCAL COLETA DESKTOP, bem como dos demais anexos a serem encaminhados eletronicamente ao TCE/RN, conforme regras e prazos estabelecidos em Resolução; o Manual de Utilização do Sistema e Manual de Preenchimento dos Anexos; e layouts de arquivos de importação, demonstradores da estrutura de arquivos a serem importados pelo referido programa.

O portal do gestor, considerando o que o TCE/RN tem a observar relativo à aplicação da LGPD consiste, pois, na *interface* entre aquele órgão fiscalizador e os seus 855 (oitocentos e cinquenta e cinco) jurisdicionados cadastrados, eis que se trata, em essência, na porta de entrada de dados no ambiente de rede do TCE/RN.

O TCE/RN disciplina por meio da Portaria n° 70[196], de 28 de fevereiro de 2019, as instruções gerais e os procedimentos pertinentes à operacionalização do Portal do Gestor, com vistas à padronização tanto do modo de acesso quanto de utilização do mesmo, para efeito de consultas e de envios de documentos, dados e informações ao Tribunal de Contas, inclusive os relativos ao SIAI.

A retromencionada Portaria obriga a todas as unidades jurisdicionadas (estadual ou municipal) a apresentarem pedido de cadastramento junto ao Portal do Gestor, por meio de ofício endereçado ao Tribunal de Contas, ao qual deverá ser anexada documentação comprobatória da sua existência (lei de criação ou de autorização, estatuto, decreto de descentralização etc.). A análise e o cadastramento do referido pleito é de competência da Secretaria de Controle Externo – SECEX, ouvidas as unidades técnicas pertinentes, caso necessário. Em caso de extinção de determinada unidade jurisdicionada, farse-á obrigatório o pedido de exclusão do seu cadastramento junto ao Portal do Gestor, mediante ofício endereçado ao Tribunal de Contas pelo titular do órgão ou entidade a que se achava vinculada a

[195] O Portal do Gestor consiste em ambiente disponibilizado pelo Tribunal de Contas do Estado do Rio Grande do Norte, com a finalidade de, via Internet, possibilitar a interação com as suas unidades jurisdicionadas. Disponível em: <www.tce.rn.gov.br> . Acessado em: 20 de mar. 2020.

[196] PORTARIA Nº 070/2019 – GP/TCE - disciplina as instruções gerais e os procedimentos pertinentes à operacionalização do Portal do Gestor do Tribunal de Contas do Estado do Rio Grande do Norte, com vistas à padronização tanto do modo de acesso quanto do de utilização do mesmo, para efeito de consultas e de envios de documentos, dados e informações ao Tribunal de Contas, inclusive os relativos ao Sistema Integrado de Auditoria Informatizada – SIAI. Disponível em: < www.tce.rn.gov.br>. Acessado em: 20 de mar. 2020.

respectiva unidade, devendo ao mesmo ser anexado via do ato normativo por meio do qual se operou a extinção.

A título ilustrativo, posto que, segundo a LGPD, os dados devem ser tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, é interessante explicitar, resumidamente, quais procedimentos a supra referida Portaria estabelece relativamente à alimentação de dados no portal do gestor pelos seus usuários.

De acordo com a Portaria, o acesso ao Portal do Gestor, relativamente a cada unidade jurisdicionada, ficará restrito a usuário previamente por ela cadastrado junto ao Tribunal de Contas. Ao disciplinar o cadastramento de usuários, a Portaria traz três definições, no § 1° do art. 7°, *in verbis: "§ 1º Para fins desta Portaria, define-se como: I - Usuário de Sistema: pessoa física vinculada a uma unidade jurisdicionada, cadastrada no Portal do Gestor e habilitada a enviar, em meio eletrônico, documentos, dados e informações ao TCE-RN conforme art. 30 da Resolução n° 011/2016-TCE; II - Usuário Gerenciador: Usuário de Sistema que, além de suas atribuições, cadastra e desabilita outros Usuários de Sistema e atribui perfis a estes; III - Perfil: combinação de permissões dada a um usuário em determinado sistema".*

A seu turno, o § 2º e o § 3º do mesmo art. 7º estabelece critérios quanto à escolha de usuários, a qual deverá recair unicamente sobre: I - agente político diretamente vinculado à respectiva unidade; II – agente público, efetivo ou comissionado, pertencente ao seu quadro de pessoal; III – agente público cedido de outra unidade da Administração Pública, independentemente da esfera governamental; e IV – em caráter excepcional, devidamente justificado, pessoa contratada para a prestação de serviços técnicos profissionais especializados no âmbito da unidade pertinente, nas áreas da engenharia e da arquitetura. Além diss, deverá ser guardada estreita correlação entre o nível funcional de cada usuário e as operações às quais o mesmo terá acesso no referido Portal.

Em atenção aos citados dispositivos, o representante legal da Unidade Jurisdicionada (Governador, Prefeito, Secretário etc) deverá designar o "usuário gerenciador" mediante portaria devidamente publicada em Diário Oficial e solicitar ao TCE-RN, por meio de *link*[197] específico do sítio eletrônico do Tribunal de Contas, o cadastramento deste no Portal do Gestor que ficará sujeita a análise e validação do TCE/RN, esta feita pela Diretoria de Informática, em conjunto com a Secretaria de Controle Externo - SECEX. O "usuário gerenciador" tem a atribuição de cadastrar e/ou desabilitar os demais usuários do sistema vinculados àquela Unidade Jurisdicionada.

[197] Cfe. O cadastramento do usuário gerenciador será feito por meio do Portal do TCE/RN. Disponível em: <http://portaletce.tce.rn.gov.br/#/servicos>. Acessado em: 02 de abr. de 2020.

Conforme visto no corpo deste trabalho, tanto a LGPD quanto o RGPD se dedicam à proteção de pessoas naturais, seres humanos, contra o tratamento ilegal de dados pessoais realizados por qualquer pessoa, seja ela outra pessoa natural, seja ela uma pessoa jurídica (ou pessoa coletiva) de direito público ou de direito privado. Importa-nos tratar da proteção de dados realizado por pessoas jurídica de direito público, no caso o TCE/RN, o TCE/PB e o TC. de Portugal e, neste tópico, apenas o primeiro deles.

Tendo em conta que a alínea "d" do inciso III do art. 4° da LGPD excetua a aplicação de seus dispositivos às atividades de investigação, e que o art. 23 condiciona o tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no art. 1° da Lei de Acesso à Informação ao atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, verifica-se que a Portaria n° 70/2019 traz em seu conteúdo alguns requisitos relativos ao supra mencionado usuário gerenciador, visando justamente por-se em adequação às exigências da LGPD, sem prejuízo do atendimento as suas atribuições legais de órgão de controle externo fiscalizador.

Com efeito, dispõe a Portaria 70/2019 que cada Unidade Jurisdicionada poderá ter até no máximo 2 (dois) usuários gerenciadores cadastrados, caso em que o cadastramento de um novo usuário gerenciador para a mesma Unidade Jurisdicionada dependerá da destituição de um deles. Contudo, o representante legal da Unidade Jurisdicionada poderá destituir o usuário gerenciador mediante portaria publicada em Diário Oficial e solicitar ao TCE-RN, por meio de link específico do sítio eletrônico do Tribunal de Contas (www.tce.rn.gov.br), a destituição deste no Portal do Gestor. A solicitação de destituição será feita mediante inserção e assinatura eletrônica da portaria mencionada e será atendida automaticamente pelo sistema.

Em relação ao usuário de Sistema, como visto nas linhas antecedentes, o TCE atrubui ao usuário gerenciador o respectivo cadastramento, por meio de *link* específico no Portal do Gestor, podendo este atribuir um ou mais perfis, guardada estreita correlação entre o nível funcional daquele e as operações às quais terá acesso no referido Portal. Com o objetivo de não travar as operações e em respeito ao Princípio Administrativo da Continuidade do Serviço Público[198], a Portaria estipulou que não há limitação do número de usuários de sistema cadastrados por Unidade Jurisdicionada. Ademais, em caso de alteração dos dados cadastrais dos Usuários de Sistema, esta poderá ser realizada pelo próprio ou pelo Usuário Gerenciador sem necessidade de autorização prévia do TCE-RN, porém a destituição ou

[198] Segundo Rivero e Waline: "*O serviço público responde, por definição, a uma necessidade de interesse geral; ora, a satisfação do interesse geral não poderia admitir a descontinuidade; toda interrupção traz o risco de introduzir, na via da coletividade, os transtornos os mais graves. Ajurisprudência construiu então o princípio da continuidade do serviço público, em virtude do qual o funcionamento do serviço não pode tolerar interrupções*." In: "*Os princípios fundamentais do serviço público"*. Droit Administratif , Précis Dalloz, 14 édition, 1992, p. 388/389.

desligamento do Usuário de Sistema poderá ser efetivada, a qualquer tempo, pelo representante legal da Unidade Jurisdicionada, com o auxílio do Usuário Gerenciador designado. Em todo caso, o TCE não exige portarias de designação ou destituição de Usuário de Sistema, eis que a atuação deste limitar-se-á a respectiva Unidade Jurisdicionada.

O Art. 14 da Portaria traz importante regra no tocante ao cadastramento de dados pelos usuários das unidades jurisdicionadas, decerto fruto da assimetria de poder na relação entre seus titulares e o Poder Público e, ainda mais, pelo fato de o Art. 25 da LGPD dispor que "os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral". Em virtude disto, o usuário que der causa ao cadastramento de dados falsos ou incompletos sujeitar-se-á, quando for o caso, a cominações legais, nas esferas administrativa, civil e penal.

A disciplina do acesso do usuário de sistema ao Portal do Gestor é também delineada de forma detalhada pela Portaria dos Art. 15 e seguintes até o Art. 18. De acordo com estes dispositivos, o usuário de sistema receberá, por meio do endereço de correio eletrônico cadastrado, uma senha provisória de acesso ao Portal, a qual é de uso pessoal e intransferível, podendo ser alterada a qualquer momento, a partir de sua alteração no primeiro acesso pelo seu detentor exclusivo, sem prévia autorização do TCE-RN. Quando do primeiro acesso do usuário por meio da senha provisória, o agente deverá ler e aceitar as condições dispostas no "termo de responsabilidade para uso do portal do gestor", nos termos do Art. 19.

A senha tornar-se-á inativa sempre que seu detentor deixar de acessar o Portal do Gestor por um período superior a 90 (noventa) dias, hipótese esta não aplicável ao usuário gerenciador.o qual detem a prerrogativa de reativar o usuário de sistema, uma vez deflagrada a situação de inatividade do acesso. Vale salientar que o usuário responderá integralmente por eventuais abusos cometidos em razão da utilização da sua senha, e poderá incorrer em cominações legais, nas esferas administrativa, civil e penal.

Por fim, quando da remessa eletrônica ou anexação de documentos ao sistema, há de serem observados os requisitos estabelecidos na Portaria n° 70/2019, quais sejam: formato PDF (*Portable Document Format*); tamanho máximo de 2 MB (mega bytes) por arquivo; assinado digitalmente, com base em certificado digital pessoa física, emitido por autoridade certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICP - Brasil[199], de acordo com as disposições normativas sobre a matéria.

[199] ICP Brasil. ICP Brasil, ou Infraestrutura de Chaves Públicas Brasileira, é, na definição oficial, "uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão". Disponível em: <https://www.iti.gov.br/icp-brasil>. Acessado em: 04 de abr. 2020.

Em nível interno, o TCE/RN promove o cadastro individual de seus servidores, atribuindo-lhes uma senha privativa de acesso ao sistema, porém define perfis de acesso hierarquizados de acordo com o cargo a ser ocupado e o nível de responsabilidade decorrente de suas atribuições. Os dados cadastrados pelos seus servidores ficam armazenados em um banco de dados da Diretoria de Informática, e são compartilhados com a Diretoria Geral de Administração sob a égide de quem se acha subordinada a Coordenação de Recursos Humanos.

É oportuno ressaltar que a LGPD traz uma lógica, ao destacar em seu art. 25, *in fine*, a necessidade de que os dados sejam mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à disseminação e ao acesso das informações pelo público em geral, a qual, segundo Cots e Oliveira[200], "[...] *a lógica empregada é que o formato não seja fechado, a fim de propiciar o tratamento dos dados pelos entes públicos das mais diferentes realidades e portes orçamentários, incluindo o compartilhamento entre eles".* A legislação vigente à que se baseia o TCE/RN, com vistas a materializar sua missão institucional, notadamente as regras previstas na Lei Ordinária Federal n.º 8.429/1992 (Lei de Improbidade Administrativa) e na Lei Ordinária Federal nº 8.730/1993[201], ensejou a edição da Resolução nº 030/2016-TCE-RN[202] que, com subsídio em ferramenta desenvolvida pela Controladoria do Município de São Paulo, regulamentou a importação do Sistema de Registro de Bens dos Agentes Públicos (SISPATRI), adaptando-o às necessidades locais.

Trata-se de um sistema que requer um fututro aperfeiçoamento e necessária adequação ao supra mencionado art. 25, além da obrigatoriedade de observância dos princípios exigidos pela LGPD, posto que interfere diretamente em dados que dizem respeito à privacidade do indivíduo. Sua abrangência alcança não apenas os servidores e membros do próprio Ttibunal de Contas, senão vejamos.

O envio das declarações é feito anualmente, até o dia 31 de maio, por meio do *link*[203] disponibilizado pelo Tribunal de Contas, sendo obrigatório para detentores de cargos eletivos, como a governadora, prefeitos, deputados e vereadores, além de membros e servidores do TCE, membros do Ministério Público Estadual (assim como todos quantos exerçam cargos, empregos ou funções de

---

[200] COTS, Marcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais comentada*. 2. ed. – São Paulo: Thomson Reuters Brasil, 2019. P. 145.

[201] Estabelece a obrigatoriedade da declaração de bens e rendas para o exercício de cargos, empregos e funções nos Poderes Executivo, Legislativo e Judiciário, e dá outras providências.

[202] Além de permitir o cumprimento, por parte dos agentes públicos municipais, da obrigatoriedade prevista nos referidos normativos de apresentação de declaração de bens e valores para a posse e exercício de mandatos, cargos, funções ou empregos nos Órgãos da Administração Direta e Indireta, o SISPATRI é de fundamental importância para o acompanhamento de suas evoluções patrimoniais, atribuição esta de responsabilidade do TCE-RN, consoante dispõe o art. 1º, inciso XXIX da Lei Complementar Estadual nº 464/2012. Disponível em: <http://www.tce.rn.gov.br/SisPatrimonio/Index>. Acessado em: 05 de abr. de 2020.

[203] Para acesso ao público por meio do *link*: Disponível em: <https://sispatri.tce.rn.gov.br/PaginasPublicas/login.aspx>. Acessado em: 05 de abr. de 2020.

confiança na instituição), secretários de estado e municípios, magistrados, e ocupantes de cargos de direção em autarquias, fundações e empresas públicas, e defensores públicos do Estado.

O aludido SISPATRI, além de permitir o cumprimento, por parte dos agentes públicos municipais, da obrigatoriedade prevista nos referidos normativos de apresentação de declaração de bens e valores para a posse e exercício de mandatos, cargos, funções ou empregos nos Órgãos da Administração Direta e Indireta, é de fundamental importância para o acompanhamento de suas evoluções patrimoniais, atribuição esta de responsabilidade do TCE-RN, consoante dispõe o art. 1º, inciso XXIX da Lei Complementar Estadual nº 464/2012[204] - Lei Orgânica do Tribunal de Contas do Estado do Rio Grande do Norte.

Por fim, cabe salientar que o subsistema que abrange o "módulo recepção", o "módulo análise" e o "módulo divulgação", que são viabilizadores do tratamento a ser dispensado pelo Tribunal aos documentos, dados e informações efetivamente coletados está em pleno desenvolvimento pela Diretoria de Informática, inclusive no tocante à normatização, tendo em conta os requisitos da LGPD.

Cabe-nos destacar algumas observações registradas quando da visita *in* loco, no tocante ao tratamento de dados pelos técnicos de informática: o dado a ser considerado é a menor partícula no processo da gestão do conhecimento – são registros sobre algum domínio; o TCE, ao trabalhar a questão dados/conhecimento, coleta várias informações (conjunto de dados estruturados) e gera conhecimento processando-as para aplicação de suas competências; o TCE/RN trabalha com dados estruturados (XML, formatação definida, banco de dados, json) e não estruturados (arquivos textos, diários oficiais); a característica dos dados estruturados é a existência de uma regra/padrão para o armazenamento das informações e podem ser recuperados facilmente, ao passo que os dados estruturados requer a construção de algum mecanismo especialista ou inteligente para recuperarf essas informações; a classificação , atualmente, segue a seguinte sistemática – gerador de dado, sistema que o transforma.

No estágio atual, como foi observado, o acesso aos dados acontece por meio de sistemas próprios com controle de acesso e por meio de consultas a bases de dados. A autorização ao acesso de dados ocorre da seguinte forma: internamente, os servidores devidamente autorizados por sua chefia imediata; externamente, cada jurisdicionado possui um usuário gerenciador que realiza a gestão dos seus próprios usuários com os respectivos controles de acesso, e os dados são transmitidos por meio dos sistemas disponibilizados aos jurisdicionados via Internet.

[204] Art. 1º O controle externo, a cargo da Assembleia Legislativa, é exercido com o auxílio do Tribunal de Contas do Estado, ao qual compete: XXIX - manter registro próprio das declarações de bens e respectivas atualizações dos dirigentes e servidores sujeitos à sua jurisdição, prevista nesta lei. Disponível em: <www.tce.rn.gov.br/legislação/LeisComplementaresEstaduais>. Acessado em: 05 de abr. de 2020.

4.2. TCE/PB – SAGRES

Antes de passarmos a detalhar as ferramentas de tecnologia da informação que o TCE/PB dispõe para colocar-se em sintonia com os requisitos da LGPD, vale ressaltar que o referido órgão está em fase embrionária no tocante à almejada adequação de suas normas internas aos requisitos da legislação protetiva de dados pessoais. Com efeito, conquanto o IRB tenha dado o *start* no estudo e consequente adaptação das normas internas dos Tribunais à LGPD, o TCE/PB tem um longo percurso a cumprir neste sentido. Cumpre-nos atestar o que se obteve da pesquisa realizada no TCE/PB.

O Tribunal opera com dois Sistemas distintos por meio dos quais são tratados os dados e informações: internamente, o TRAMITA, por meio do qual são alimentados os dados e gerados os processos no ambiente de rede; e o SAGRES *on lin*e, incluído a sua versão SAGRES *captura*[205] – que é o Sistema de Acompanhamento de Gestão de Recursos da Sociedade, cujas funcionalidades são específicas para atuação dos Tribunais de Contas, atualmente operável em vários Estados da Federação, e que dispõe de um Portal do Jurisdicionado, cujo objetivo é servir como canal de comunicação entre o TCE-PB e os Órgãos Jurisdicionados.

O SAGRES trabalha com dados abertos[206], uma linha de pensamento inteiramente compatível com o princípio da transparência pública, propugnado pela lei de acesso à informação, o que faz o TCE-PB disponibilizar algumas tabelas do banco de dados do SAGRES, na forma de dados abertos.

Assim sendo, qualquer pessoa pode baixar os dados disponíveis, ficando livre para fazer qualquer tipo de tratamento neles. Neste sentido, resta claro que o TCE-PB não será responsável por nenhum tipo de processamento feito nesses dados, o que enseja um profundo ajuste nesta ferramenta com vistas à adequá-la à LGPD, eis que alguns dos dados a serem tratados pelo Tribunal de Contas merecem a devida proteção por se constituírem em um direito de seus titulares. Há de segregar, portanto, os dados que podem ser mantidos à luz da lei de acesso à informação, em observância aos princípios da transparência e da publicidade e os dados pessoais, de seus titulares, os quais ensejarão os respectivos consentimentos, nos termos da LGPD.

Por assim ser concebido, ou seja, para trabalhar com dados abertos, e visando facilitar o acesso dos usuários jurisdicionados, as tabelas do SAGRES disponíveis para download estão no formato texto,

---

[205] O Sistema de Acompanhamento da Gestão dos Recursos da Sociedade (SAGRES) na versão Captura é um módulo que permite a captura dos dados da execução orçamentária, licitações, obras e folha de pessoal dos jurisdicionados que devem enviar a prestação de contas públicas ao TCE. Disponível em: <https://tce.pb.gov.br/servicos/sagres-captura> . Acessado em: 14 de abr. de 2020.

[206] Segundo a Open Knowledge Foundation, "dados são abertos quando qualquer pessoa pode livremente usá-los, reutilizá-los e redistribuí-los, estando sujeito a, no máximo, a exigência de creditar a sua autoria e compartilhar pela mesma licença". Disponível em: <www.tce.pb.gov.br/serviços/dados-abertos> . Acessado em: 14 de abr. 2020.

UTF-8, compactado com GZip. As colunas estão separadas por caracteres *pipe* ('|') e as linhas, por caracteres de nova linha, '\n'. A primeira linha de cada arquivo texto contém os nomes das colunas da tabela, separadas por caracteres *pipe*, a fim de indicar a ordem em que as colunas aparecem no arquivo.

Os dados alimentados pelos Jurisdicionados guardam relação com a atividade-fim do Tribunal de Contas, qual seja a atribuição constitucional do exercício do controle externo de seus jurisdicionados (Prefeituras, Estado, Administração indireta etc) e constituem-se na contabilização efetuada pelas administrações, submetendo-se à análise de consistência e validação do TCE/PB, e podem ainda ser modificados quando por este auditados. Observa-se o formato interoperável e estruturado para o uso compartilhado, bem como que se presta à disseminação e ao acesso das informações pelo público em geral, nos termos do Art. 25 da LGPD. É certo, porém, que nem todas as tabelas disponibilizadas possuem atributos para os quais o TCE/PB deve estar atento às regras de tratamento de dados pessoais prescritas no capítulo IV da LGPD.

A título de exemplificação, ao acessar o sistema no sítio do TCE/PB, um prefeito municipal ou o seu representante legal por ele previamente designado e cadastrado, no intuito de cumprir suas obrigações relativas à prestação contas de determinado exercício financeiro tem a preencher as tabelas que contém informações da Receita Orçamentária, empenhos, pagamentos, estornos, licitações e folha de pessoal. Dentre estes arquivos disponibilizados, o TCE/PB deverá ater-se ao tratamento de dados pessoais, segundo a LGPD, ao verificar os atributos a serem preenchidos precipuamente na tabela de folha de pagamento, eis que nesta constam dados pertencentes a uma pessoa natural funcionário da referida prefeitura, a saber: nome, CPF, vantagens monetárias, data de nascimento, cargo que ocupa. Não se trata de tarefa tão simples, posto que deverá haver uma conformidade com os princípos da Lei de Acesso à Informação e com os requisitos da LGPD, os quais protegem os direitos do tirular dos dados pessoais e exige o seu consentimento para que se tornem públicos.

O SAGRES foi concebido para ser uma importante ferramenta de controle social, disponibilizado à sociedade para que esta possa fiscalizar a aplicação dos recursos públicos do Estado e dos municípios. Contudo, ao viabilizar o controle social e por em prática o princípio da transparência, disponibilizando, em seu site (http://portal.tce.pb.gov.br), qualquer cidadão, possua ou tenha acesso a um computador conectado à rede mundial de computadores – INTERNET, pode acompanhar a execução orçamentária do Estado e dos Municípios Paraibanos, bem como aos dados pessoais de funcionários públicos cadastrados pelos titulares de Poder, ou de quem os represente, o que vai de encontro ao objetivo de proteção dos direitos fundamentais de liberdade e privacidade e do livre desenvolvimento da personalidade da pessoa natural, nos termo do Art. 1° da LGPD.

A este respeito, vale repisar que os fundamentos previstos no Art. 2° da LGPD não faz

distinção entre pessoa de direito privado ou de direito público para seu cumprimento em relação à proteção de dados, ou seja, o respeito à privacidade, à autodeterminação informativa, à inviolabilidade da intimidade, da honra e da imagem, os direitos humanos, a dignidade e o exercício da cidadania pelas pessoas naturais devem ser observados incontestamente. E, no caso dos Tribunais de Contas, tais fundamentos hão de ser significativamente considerados, pois não se pode valer das informações prestadas quando da apresentação das contas a serem auditadas, para subverter a tais fundamentos.

Para o cumprimento destes fundamentos, o TCE/PB deverá ater-se ao que dispõe os incisos I e II do Art. 23 da LGPD, quais sejam: deverá publicar de forma clara e precisa, de preferência em seu sítio eletrônico, informações relativas ao tratamento, como a previsão legal, a finalidade, os procedimentos e práticas utilizadas no tratamento, entre outras informações; e indicar um encarregado. Contudo, é importante salientar o disposto no art. 7°, segundo o qual, por ser parte integrante da Administração Pública, o TCE/PB pode tratar dados mediante base legal específica (inciso III), não dependendo do consentimento ou enquadramento em outras hipóteses, exceto se for mais específica, ao tutelar a saúde, por exemplo.

A base técnica dos dados do SAGRES são os lançamentos detalhados em contas correntes contábeis segundo as Normas Brasileiras de Contabilidade Aplicadas ao Setor Público (NBCASP), adotando-se como padrão o Plano de Contas Aplicado ao Setor Público (PCASP) da Secretaria de Tesouro Nacional – STN, revisado periodicamente, com as seguintes características funcionais: Integridade dos dados, segurança, confiabilidade, simplicidade de procedimentos, interface amigável, padronização e validação com regras contábeis.

A fim de atender a demanda dos jurisdicionados, ao desenvolver a ferramenta, a Assessoria Técnica de Comunicação – ASTEC[207] contemplou as seguintes características técnicas[208] afetas ao SAGRES:

I - Estruturação em duas camadas: uma camada composta por um banco de dados e outra por um programa (*front end*) que seleciona, altera, processa, alimenta e/ou exclui os dados constantes da base de dados;

II - Modularidade: por se tratar de um sistema destinado a ser operado, tanto nos computadores dos jurisdicionados, como nos do Tribunal, optou-se pela divisão em três módulos interdependentes, para melhor integração, a saber:

a) Módulo Captura – o qual é fornecido gratuitamente aos jurisdicionados, cuja finalidade

[207] Setor subordinado à Presidência do TCE que tem como atribuição gerir as atividades de Tecnologia da Informação. Disponível em: <www.tce.pb.gov.br/institucional>. Acessado em: 03 de maio de 2020.

[208] SAGRES ON LINE. Disponível em: < https://tce.pb.gov.br/sagres-online>. Acessado em: 03 de maio de 2020.

é a verificação da consistência dos dados e a realização da geração, criptografia e travamento dos arquivos contendo as informações mensais a serem enviadas ao Tribunal;

b) Módulo Carga – destinado ao uso pelos funcionários da Divisão de Expediente e Comunicações do TCE/PB. que tem como objetivo receber, destravar, descriptografar e dar "carga" nos dados entregues pelo jurisdicionados;

c) Módulo Auditor – que se presta a dar suporte às atividades da área-fim desempenhadas pelos Auditores de Contas Públicas do Tribunal responsáveis pela análise da documentação encaminhada pelos jurisdicionados.

Como dito alhures, a outra ferramenta que o TCE:PB utiliza para a movimentação interna de documentos e processos em seu ambiente de rede é o TRAMITA que, como o nome sugere, presta-se às funcionalidades inerentes ao tratamento de dados e informações inerentes aos processos alimentados em seu sistema. Devido as suas funcionalidades, necessário se faz adequar o TRAMITA aos requisitos da LGPD, o que exigirá uma dedicação intensa dos técnicos da área de tecnologia da informação.

Em sua versão atual, o TRAMITA 20.2, o sistema permite tanto o acesso interno quanto o externo, sendo o primeiro permitido a todos os servidores do TCE-PB em um atalho nas suas respectivas máquinas de trabalho, bastando para isso, um clique que, instantaneamente, o sistema abrirá um navegador ditetamente do sistema ou, caso prefira, poderá ser aberto o navegador que se deseja e digitar o caminho: https://tramita. Para o acesso externo, qual seja, fora das dependências do Tribunal, necessário se faz o servidor do TCE/PB obter autorização prévia, caso em que é exigido o máximo de responsabilidade ao usar o Tramita em computadores externos, haja vista o risco de vazamento de informações e senhas.

Acerca do alegado risco de vazamento de informações e senhas, necessário se faz observar o disposto no art. 7° da LGPD, segundo o qual o Poder Público poderá realizar tratamento de dados em determinadas circunstâncias, aí incluídos a comunicação e o compartilhamento de dados com terceiros, e considerar também o §1° do Art. 26[209], onde estão previstas algumas exceções quando do

[209] Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

I- em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);

II - (VETADO)

III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei;

IV – Quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres;

compartilhamento de dados.

O TRAMITA permite aos seus usuários servidores o acesso as suas funcionalidades, o que inclui a anexação e desanexação de documentos e processos, o cancelamento de arquivos processuais, o despacho de processos e documentos, o acesso aos módulos licitações, contratos, aditivos, relatório da gestão da informação, enfim, a um elenco de dados, inclusive dados pessoais, o que torna o sistema frágil em termos de proteção dos direitos dos titulares dos dados acessados.

Cabe ressaltar, que a LGPD não inviabiliza nem tampouco altera as regras da LAI, tanto é assim que o inciso I do Art. 26 faz referência expressa neste sentido. No caso, invoca-se um elenco de direitos ao acesso à informação previstos no Art. 7° da LAI, o que requer uma melhor adequação à LGPD das funcionalidades disponíveis no TRAMITA.

A fim de se ter um noção da falta de uniformidade no tratamento de dados da forma como disposta no TRAMITA, exemplifiquemos com uma das funcionalidades a que se tem acesso. Ao clicar em "Módulos"[210], abre-se o subitem "Relatórios de Gestão da Informação", cujo atributo está assim descrito: "A solicitação de informações ao setor de Gestão da Informação (GI) e os relatórios produzidos pelo setor passarão a ser controlados pelo Tramita. As funcionalidades estarão disponíveis no menu GI na barra de menus. Inicialmente terão acesso a esse menu apenas os seguintes grupos de usuários: Conselheiros; Conselheiros Substitutos; Procuradores; Diretor de Auditoria e Fiscalização (DIAFI) e Auditores lotados na GI." Outors usuários poderão ter o acesso concedido mediante solicitação ao Suporte Tramita. Somente os usuários com acesso ao *menu* GI poderão solicitar informações ou visualizar os relatórios da Gestão da Informação.

Do texto evidenciado, verfica-se que o Tramita estabelece critérios e perfis de acesso aos relatórios gerados pelo setor de Gestão da Informação, ou seja, somente pessoas determinadas, com um grau de autoridade e responsabilidades superiores poderão solicitar informações ou visualizar os relatórios da Gesta da Informação, ante o seu caráter sigiloso. Para as demais funcionalidades não há esta exigência, o que habilita aos demais usuários acessar os dados nelas contidos, inclusive com possibilidade de compartilhar, eis que não se padronizou as regras de tratamento de dados, inclusive pessoais, nos termos da LGPD aplicável ao Poder Público, *in casu*, o TCE/PB.

Observa-se, pois, que tanto o sistema SAGRES, com suas opções de axcesso, qunato o TRAMITA ensejam uma revisão de suas funcionalidades, sob pena de se colocar em desacordo com as

---

V - hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado otratamento ;para outras finalidades. Disponível em: <www.planalto.gov.br>. Acessado em: 17 de maio de 2020.

[210] TRAMITA-SUPORTE –Tribunal de Contas da Paraíba. Disponível em: <www.tce.pb.gov/tramita>. Acessado em: 17 de maio de 2020.

regras de proteção de dados, inclusive no tocante às regras de consentimento para o qual a LGPD prevê dez bases legais para o processamento de dados pessoais, partindo do pressuposto de que o titular dos dados poderá definir antes da coleta, a seu exclusivo critério, se um agente público poderá ou não realizar quaisquer atividades de tratamento de seus dados pessoais.

A despeito disto, algumas observações merecem registro no que se refere à estrutura de tecnologia da Informação da qual dispõe o TCE/PB para alcançar a esperada adequação de suas normas às regras da LGPD. Com efeito, a Assessoria Técnica – ASTEC, setor que coordena as atividades de informática trabalha com dados estruturados no formato TXT e XML, dados de georreferenciamento no formato latitude/longitude decimal e arquivos em PDF, KML, CSV, XLSX e JPEGH. Utiliza as linguagens Scala, Java, Delphi e SQL.

Para execução de suas atribuições de TI e desenvolvimento de suas ferramentas, a ASTEC considera dados todo documento ou informação que permite, em uma análise conjunta ou isolada, chegar ao conhecimento de algo ou deduzir um facto, podendo consistir em números, palavras e imagens, medições e observações de um conjunto de variáveis. Do ponto de vista do gerador de dados, eles podem ser informados pelos jurisdicionados, produzido pelo próprio Tribunal ou informados por terceiros. Podem ser utilizados por seus técnicos ou processados por uma entrada em um computador, armazenados e então serem tratados. Ao passo que conhecimento é a ordenação, interpretação e organização destes dados, em uma análise conjunta ou isolada, de forma a transmitir significado e compreensão dentro de um determinado contexto, a exemplo das funcionalidades do TRAMITA.

Em conclusão, o TCE/PB permite o acesso aos dados pelos usuários internos e externos por meio do SAGRES e do TRAMITA, sendo que todos os servidores acessam os dados de acordo com o seu perfil. Os jurisdicionados acessam os dados dos seus respectivos municípios e Estado com o perfil de inserir a informação no formato e prazo preestabelecido em normativo próprio, as Resoluções Normativas. Os dados são transmitidos pelos jurisdicionados atraves da internet. Disponibilizado para os servidores do TCE na intranet. Disponibilizado para a sociedade atraves da internet em uma DMZ. Os servidores do TCE visualizam todos os dados e podem inseri-los somente nos processos de sua responsabilidade.

Ademais, sob o prisma da LGPD, o TCE-PB ainda não estabeleceu formalmente os agentes de tratamento de dados, sendo esta tarefa desempenhada atualmente pela ASTEC, que é o setor responsável pela guarda e gerenciamento dos dados informados e produzidos no TCE/PB.

4.3. Tribunal de Contas de Portugal – Sistema da Informação

O Tribunal de Contas de Portugal, ao contrário dos Tribunais de Contas alhures analisados, está a uma distância considerável em termos de adequação de seu Sistema de Informática, visando o atendimento dos requisitos do Regulamento Geral de Proteção de Dados.

No capítulo anterior, foi visto que, em virtude da entrada em vigor do RGPD, em 25 de maio de 2018, o PG-TC, tendo em conta que a aplicação do RGPD fora objeto de estudos preparatórios coordenados pelo Departamento de Consultoria e Planejamento, aprovou a Resolução n° 3/2018-PG, de 28 de maio de 2018, por meio da qual adotou duas medidas iniciais fundamentais: i) a adequação da publibcitação do conteúdo dos atos do Tribunal ao princípio da minimização de dados; e ii) a designação de um Encarregado de Proteção de Dados e a definição do seu estatuto. Esta última medida já foi objeto de análise no capítulo III.

A tais medidas outras serão acostadas, notadamente em virtude da apreciação e aprovação da Proposta de Lei n° 126/XIII encaminhada à Assembleia da República, visando à adaptação de algumas de suas disposições ao sistema judicial. Na prática, a iniciativa concerne à atribuição de poderes aos juízes relatores de processos e atos jurisdcionais ou de conbtrolo financeiro da competência do Tribunal de Contas, enquanto responsáveis pelo tratamento e proteção de dados no âmbito daqueles atos e processos, em articulação com a ação a desenvolver pelo Encarregado de Proteção de Dados, em atenção às atribuições e funções previstas no RGPD para este agente.

Por meio do Regulamento 112/2018[211], de 15 de fevereiro de 2018, em seu Capítulo VI, o Tribunal de Contas traça as principais disposições acerca dos objetivos, regulamentação e da Comissão de Informática, relativas ao Sistema de Informação. Antés, porém, o Capítulo IV do mesmo Regulamento dedica dois artigos à Política de Comunicação e Transparência (Publicitação dos atos), o Art. 13° e o Art. 14°, respectivamente.

O Art. 13°, ao dispor sobre a Política de Comunicação, faz referência expressa a três princípios, entre os quais o da proteção de dados pessoais, o que está em sintonia com os objetivos propostos no Art. 17°, relativamente à fiabilidade e segurança, além da utilidade e oportunidade da informação, requisitos estes presentes no RGPD Europeu. De acordo com o Art. 13°: "O *Tribunal de Contas define uma estratégia de comunicação, adequada ao cumprimento do seu mandato, com observância dos princípios da transparência, da prestação de contas e da proteção de dados pessoais,*

[211] Dispõe sobre o Regulamento do Tribunal de Contas (RTC), em complemento à Lei de Organização e Processo do Tribunal de Contas de Portugal (LOPTC). Disponível em: <https://www.tcontas.pt/pt-pt/TribunalContas/Publicacoes/ColetaneasLegislacao/Pages/detalhe.aspx>. Acessado em: 23 de maio de 2020.

designadamente através da divulgação do resultado dos seus trabalhos em tempo oportuno". No retrocitado Regulamento, nos termos do Art. 17.º, o Tribunal explicita os quatro objetivos[212] a que se presta o Sistema de Informação, sem olvidar, contudo, das disposições a serem observadas no que concerne à política de Comunicação.

Atento ao disposto nos supracitados Artigos 13° e 17°, o Departamento de Sistemas e Tecnologias de Informação (DSTI), setor subordinado à Direção-Geral do Tribunal de Contas (DGTC), como já referenciado no corpo deste trabalho, tem a incumbência de tornar o Sistema de Tecnologia da Informação um garantidor dos objetivos alinhados no Art. 17°, e contemplar, no mínimo, as orientações previstas em Regulamento de competência do Presidente do Tribunal de Contas de Portugal, segundo dispõe o Art. 18°[213].

As disposições legais e regulamentares previstas no número 2° do Art. 18° , para a qual o Sistema de Informação deve observância, são as regras contidas no RGPD, daí o motivo pelo qual o Tribunal de Contas fez constituir uma Comissão de Informática[214] permanente, cujas competências estão

---

[212] Artigo 17.º

Objetivos

O Tribunal de Contas dispõe de um sistema de informação integrado e interativo, com vista a garantir:

a) A otimização dos recursos, designadamente em termos de informação a produzir, seu conteúdo, normalização e distribuição;

b) A utilidade e a oportunidade da informação;

c) A fiabilidade da informação;

d) A segurança da informação.

Disponível em: < https://www.tcontas.pt/pt-pt/TribunalContas/Publicacoes/ColetaneasLegislacao/Pages/detalhe.aspx>. Acessado em: 13 de maio de 2020.

[213] Artigo 18.º

Regulamentação

1. O sistema de informação é regulamentado pelo Presidente tendo em conta as orientações gerais definidas pelo Plenário Geral, e deverá contemplar:

a) A identificação do gestor ou responsável pelo sistema e definição das respetivas funções;

b) A definição de níveis de acesso à informação para efeitos de registro e consulta;

c) A definição de níveis de gestão da rede;

d) A criação de indicadores de alerta que identifiquem tentativas de intrusão e respetiva origem;

e) A definição de critérios gerais e níveis de competência relativos à disponibilização de informação para o exterior.

2. A regulamentação do sistema de informação deverá ainda respeitar as disposições legais e regulamentares relativas à proteção de dados pessoais.

Disponível em: < https://www.tcontas.pt/pt-pt/TribunalContas/Publicacoes/ColetaneasLegislacao/Pages/detalhe.aspx>. Acessado em: 13 de maio de 2020.

[214] Artigo 19.º

Comissão de Informática

1. O sistema de informação é acompanhado permanentemente por uma Comissão de Informática presidida por um Juiz Conselheiro eleito pelo Plenário Geral, por um magistrado do Ministério Público, pelo gestor ou responsável pelo sistema de informação e por um técnico dos Serviços de Apoio nomeado pelo Presidente.

Disponível em: <https://www.tcontas.pt/ptpt/TribunalContas/Publicacoes/ColetaneasLegislacao>. Acessado em: 13 de maio de 2020.

definidas no número 2 do Art. 19° do Regulamento 112/2018, de 15 de fevereiro de 2018 e, especificamente em relação à proteção de dados, a alínea c), do n° 2 do Art. 19°, fez expressamente menção no sentido de que compete à retrocitada Comissão "[...] *assegurar o cumprimento dos dispositivos legais, designadamente relativos à proteção de dados pessoais".*

Incumbe, ainda, a referida Comissão de Informática, que tem a função de acompanhar as ações desenvolvidas pelo Sistema de Informação, entre outras competências: zelar para que a informação produzida seja completa, útil e relevante, fiável, oportuna e segura; ser ouvida sobre a informação a produzir, designadamente sobre o seu conteúdo, normalização e forma de tratamento; além de ser ouvida sobre a segurança da informação, especialmente sobre o seu nível, grau de confidencialidade, qualidade dos seus suportes e classificação dos documentos.

A par disso, com base na mencionada Resolução n° 3/2018-PG, de 28 de maio de 2018, e em conformidade com o Art. 13°, a Comissão de Informática e o Departamento de Sistemas e Tecnologias de Informação (DSTI) envidaram esforços no sentido de garantir que os atos publicados pelo Tribunal de Contas não contivessem informações pessoais que vão para além do necessário, atendendo ao interesse público prosseguido com a respectiva publicação. Para estar em confirmidade com esta diretriz, alguns procedimentos de adequação foram contemplados pelo sistema de informação, notadamente aqueles já descritos no item 3.3 do capítulo anterior deste trabalho, os quais se faz oportuno repisá-los a seguir:

- Aos serem publicados, os acórdãos, sentenças, relatórios de auditoria e outros atos do Tribunal, assim como os atos do Ministério Público neles integrados devem conter apenas os dados pessoais indispensáveis à informação da sociedade sobre a utilização dos recursos financeiros públicos e à garantia da *accountability* dos gestores desses recursos e dos responsáveis financeiros;

- Adotando-se o princípio da ponderação no confronto entre o interesse público prosseguido e o direito de proteção de dados pessoais, ao publicar os atos do Tribunal, deve-se considerar legítima, adequada, necessária e proporcional, a explicitação do nome e cargo das pessoas em causa, desde que sujeitos à jurisdição do Tribunal, devendo ser omitidos outros dados pessoais, exceto se ficar demonstrada a relevância pública destes atos;

- É preciso levar em conta a eventual desnecessidade de referências na publicitação dos atos do Tribunal a empresas ou outros sujeitos privados, singulares ou coletivos, de relações jurídicas com entidades públicas sujeitas à jurisdição do Tribunal e que não tenham qualquer responsabilidade pela gestão ou pela utilização de dinheiros ou ativos públicos;

- Atribui-se ao Juiz Conselheiro relator a responsabilidade de identificar os dados pessoais que

devam ser omitidos e, caso haja dúvida sobre os dados pessoais que podem constar na publicação dos atos, esta deverá ser dirimida mediante consulta ao Encarregado de Proteção de Dados do Tribunal de Contas.

Definidos os principais procedimentos a serem observados pelo Sistema de Informação e Tecnologia, visando garantir que os atos publicados pelo Tribunal não contém informações pessoais desnecessárias e não consentidas pelo titular, nos termos da RGPD, é de bom alvitre discorrer, de forma sintética, como se apresenta e se comunica com à sociedade o Sistema de Informação do Tribunal.

Ao tecer comentários ao Art. 17°, foi visto que o Tribunal de Contas dispõe de um Sistema de Informação Interativo e integrado, com vista a garantia dos princípios de proteção de dados. Em sua estrutura, vimos que o setor responsável pelo desenvolvimento de ferramentas de tecnologia da Informação e demais atribuições correlatas é o Departamento de Sistemas e Tecnologias de Informação (DSTI)[215], nos termos do número 1 do Art. 8°, do Regulamento de Organização e de Funcionamento da Direção-Geral do Tribunal de Contas (ROF-DGTC).

Neste norte, é importante fazer uma distinção relativa aos Sistemas e Tecnologia de Informação do Tribunal de Contas. As atividades do Departamento de Sistemas e Tecnologias de Informação (DSTI) são de amplo escpectro, vale dizer, o Sistema de TI contempla ferramentas que se prestam à comunicação tanto internamente quanto externamente, cujas informações são acessíveis também aos cidadãos.

Contudo, o Regulamento de Organização e de Funcionamento da Direção-Geral do Tribunal de Contas (ROF-DGTC), Despacho n° 9675/2000, de 10 de maio de 2000, no n° 4 do Art. 1°, traz em seu conteúdo a criação do Núcleo de Apoio Técnico ao Desenvolvimento de Auditorias dos Sistemas Informáticos e em Ambiente Informático (NATDA), diretamente dependente da Direção-Geral, cujo cargo é ocupado por um Juiz-Conselheiro. Este último contempla o suporte às auditorias dos sistemas informáticos, notadamente direcionado as atribuições desempenhadas na atividade fim pelos fiscalizadores sobre os sistemas de tecnologia das Entidades Fiscalizadas.

Vale ressaltar que o DSTI, devido a sua abrangência de atuação, funciona igualmente em estreita articulação com o Núcleo de Apoio Técnico ao Desenvolvimento de Auditorias dos Sistemas Informáticos e em Ambiente Informático (NATDA), disponibilizando programas, desenvolvendo

[215] Artigo 8.º

Departamento de Sistemas e Tecnologias de Informação (DSTI)

O DSTI é o departamento de apoio instrumental que tem por missão a conceção e permanente adaptação dum sistema integrado de gestão e informação para utilização do Tribunal e dos Serviços de Apoio, compreendendo, nomeadamente, subsistemas de gestão de entidades e de gestão processual, incumbindo-lhe, designadamente.

Disponível em: <https://www.tcontas.pt/ptpt/TribunalContas/Publicacoes/ColetaneasLegislacao>. Acessado em: 03 de maio de 2020.

aplicativos, máquinas e equipamentos de informática, etc.

Tendo em conta que os diversos setores do Tribunal de Contas atuam de forma integrada[216] (conforme o n° 10, do Art. 11° do ROF-DGTC), objetivando a execução de sua atividade fim, o Serviço de Gestão de Entidades (SGE)[217], que tem como missão a coordenação do sistema de gestão de entidades (GENT), tem entre as suas atribuições, a de garantir a organização e atualização permanente da base de dados das entidades sujeitas à jurisdição e ao controlo do Tribunal de Contas, bem como criar e manter atualizados os processos respectivos com todas as informações disponíveis, com vista à sua utilização, nomeadamente pelos departamentos de apoio técnico-operativo, sem prejuízo das bases de dados especializadas de que estes careçam, com vista à organização dos dossiers permanentes das entidades integradas no respectivo domínio de controlo.

Em contrapartida, o DSTI tem, entre as suas atribuições, o dever de colaborar com o Serviço de Gestão de Entidades (SGE) na concepção e manutenção de um sistema integrado de gestão das entidades sujeitas ao controlo do Tribunal de Contas, nos termos da alínea "f", do número 1 do Art. 8° do Regulamento da Organização e de Funcionamento da Direção Geral do Tribunal de Contas (ROF-DGTC).

O atual sistema de tecnologia da Informação do Tribunal de Contas de Portugal contempla as aplicações informáticas disponibilizadas ao acesso de seus usuários internos e externos, sendo estes últimos as Entidades jurisdicionadas ou fiscalizadas[218] no âmbito da atividade fim.

Para fazer face ao cumprimento legal e regulamentar de suas exigências pelos seus fiscalizados, o Tribunal disponibiliza o Sistema "econtas", por meio do qual o usuário externo acessa uma área pública de "Serviços *online do TdC",* onde se encontram os *links* necessários à comunicação

---

[216] Artigo 11.°

Secretaria do Tribunal (ST)

10. Todos os Serviços devem colaborar com as informações de que disponham relativamente às entidades sob a jurisdição e o controlo do Tribunal, de acordo com as orientações estabelecidas por despacho do Diretor-Geral. Disponível em: <https://www.tcontas.pt/ptpt/TribunalContas/Publicacoes/ColetaneasLegislacao>. Acessado em: 10 de maio de 2020.

[217] Artigo 11.º

Secretaria do Tribunal (ST)

1. A ST é o departamento de apoio instrumental que tem por missão garantir o apoio administrativo e processual inerente ao funcionamento do plenário geral, da comissão permanente e das secções especializadas, bem como assegurar o sistema de gestão de entidades

2. A ST compreende a Divisão de Apoio Processual, organizada em Núcleos de acordo com as suas missões, bem como o Serviço de Gestão de Entidades (SGE). Disponível em: < https://www.tcontas.pt/ptpt/TribunalContas/Publicacoes/ColetaneasLegislacao>. Acessado em: 10 de maio de 2020.

[218] O número de entidades registradas no Tribunal de Contas, considerando as duas Secções de Açores e da Madeira é de 7373. O número de entidades alvo da fiscalização é de 6123. Fonte: www.econtas.tcontas.pt. Consultado em 03/06/2020. Disponível em: <https://www.tcontas.pt/ptpt/TribunalContas/Publicacoes/>. Acessado em: 21 de maio de 2020.

das informações a serem prestadas relativas às prestações de contas e demais dados requisitados. A página inicial do Sistema também disponibiliza alguns indicadores, em conformidade com o princípio da transparência, além ofertar suporte técnico, downloads do manual do utilizador (prestação de contas, fiscalização concomitante), documentos de referência e dados estatísticos das entidades prestadoras.

Por meio do "*econtas*" o Tribunal garante a operacionalidade de seu sítio eletrônico, cujo conteúdo é da responsabilidade do Departamento de Consultoria e Planejamento – DCP[219], nos termos de despacho do Presidente, com proposta do Diretor-Geral, e após ouvir a Comissão de Informática. O pessoal ocupante de cargos (técnicos verificadores, assistentes, diretores, chefes de divisão etc) também têm acesso ao sistema, posto que são previamente cadastrados por matrícula e lhes são fornecidos a palavra-chave (senha) individual. Ademais, as respectivas senhas individuais lhes dão acesso à rede interna do Tribunal-Intranet, possibilitando a navegação, comunicação com os departamentos, solicitação de documentos, preenchimento de formulários ao departamento de recursos humanos entre outras ferramentas restritas ao ambiente interno de rede.

O referenciado serviço *online* têm o objetivo de possibilitar a entrega e consulta de contas de gerência por meios eletrónicos por parte dos serviços e organismos sujeitos à jurisdição e controlo do Tribunal de Contas, além do envio de dossiês de adicionais, que viabiliza a remessa e consulta, por via eletrónica, de atos ou contratos que titulam modificações a contratos de empreitada já visados pelo Tribunal de Contas relativas a trabalhos a mais, de suprimento de erros e omissões ou complementares.

Este Sistema permite três grandes níveis de sustentabilidade: i) ao nível da informação, para que esta se apresente de uma forma mais disponível e com uma maior possibilidade de utilização; ii) ao nível do controlo, permite uma maior qualidade da conta de gerência, redução do tempo médio de análise por processo e controlo eficiente dos processos; e iii) ao nível da transparência, permite redução do "preço" por processo, maior clareza dos processos e interfaces com soluções de apoio à gestão de terceiros. (Consultado em TC de Portugal/Publicações, 2019)

---

[219] Artigo 5.º

Departamento de Consultadoria e Planeamento (DCP)

1. O DCP tem por missão assegurar as funções de estudo e de investigação para apoio aos sistemas de fiscalização e controlo, de apoio aos sistemas de fiscalização e controlo, de apoio ao planeamento das atividades e às relações internacionais do Tribunal e de tratamento de informação, competindo-lhe, designadamente:

a) ..

[...]

i) Assegurar, com a colaboração do DSTI e de acordo com as orientações constantes de despacho do Presidente, sob proposta do Diretor-Geral, ouvida a Comissão de Informática, o conteúdo do site do Tribunal de Contas na Internet, em língua portuguesa e com sumário em inglês, permanentemente atualizado, sendo a operacionalidade em rede garantida pelo DSTI. Disponível em: < https://www.tcontas.pt/ptpt/TribunalContas/Publicacoes/ColetaneasLegislacao> . Acessado em 03/06/2020.

A adesão das entidades aos referidos serviços online não comporta quaisquer custos adicionais, sendo exigido tão somente a instalação e manutenção de uma ligação à Internet, além do preenchimento do pedido de adesão em formulário *online*, ocasião em que o sistema gerará os seguintes dados: Identificação do cadastrado e uma palavra-chave (senha de acesso). O sistema fornecerá também um segundo código de acesso para a validação final da conta a entregar por parte do dirigente de último nível – o código de acesso para entrega da conta de gerência.

Ao selecionar a opção "Pedido de Adesão" na página inicial do sistema, abre-se o formulário *online*, o qual requer o preenchimento dos dados necessários ao registro, quais sejam: a identificação do utilizador que faz o pedido; a identificação da entidade; a função / categoria do utilizador; o endereço de correio eletrónico do utilizador; a morada / endereço postal da entidade; a localidade postal da entidade; e o código postal da entidade. Contudo, o preenchimento e entrega destes dados não conferem automaticamente a criação de uma conta de utilizador no sistema, porquanto deverão ser submetidos à análise e, em seguida, validados pelo Tribunal de Contas para, posteriormente, serem enviados pelo correio com endereçamento ao órgão máximo da entidade. Vale salientar que o sistema bloqueia o acesso, após o utilizador errar por três vezes consecutivas o preenchimento da palavra-chave, a qual poderá ser recuperada mediante o acesso à opção "recuperar palavra-chave" constante na página inicial na área de registro e entrada. (Consultado em TC de Portugal/Publicações, 2019)

Após acessar devidamente o sistema, o utilizador poderá preencher os documentos da prestação de contas através da importação de ficheiros em formato XML, os quais deverão obedecer a estruturas específicas. Estas estruturas (*XML Schema Definition*) estão organizadas por regime contabilístico e forma de entrega, permitindo fazer *downloads* (descarregamento) para obtenção dos modelos. Ademais, há a opção dos documentos XML a remeter serem validados diretamente a partir do URL[220] de acesso público https://econtas.tcontas.pt/extgdoc/extgdoc/schema.

Ao referir-se aos três níveis de sustentabilidade permitidos pelo sistema, foi explicitado que o nível do controlo permite uma maior qualidade da conta de gerência, uma redução do tempo médio de análise por processo e num controlo eficiente dos processos. Em relação a esta conta de gerência, o sistema disponibiliza uma opção de cadastramento e acesso a funcionalidades diferenciadas, sobre as quais dedicar-se-á breves linhas.

[220] URL é o endereço de um recurso disponível em uma rede, seja a rede internet ou intranet, e significa em inglês *Uniform Resource Locator*, e em português é conhecido por Localizador Padrão de Recursos. Em outras palavras, URL é um link endereço virtual com um caminho que indica onde está o que o usuário procura, e pode ser tanto um arquivo, como uma máquina, uma página, um site, uma pasta etc. Um URL é composto de um protocolo, que pode ser tanto HTTP, que é um protocolo de comunicação, FTP que é uma forma rápida de transferir arquivos na internet etc. Disponível em: < https://www.significados.com.br/url/> . Acessado em 04 de jun. de 2020.

Uma vez registrado e autenticado, o utilizador tem acesso a uma área de trabalho, na qual constam dados de natureza informativa sobre o último acesso realizado e entidade que representa, além de dispor da opção de personalização do ambiente de trabalho. O aplicativo permite ao utilizador melhorar o seu ambiente de trabalho, adaptando-o às capacidades do seu equipamento e ao seu gosto (tamanho e largura da página, tamanho da letra e cores preferidas).

A aplicação desdobra-se em duas grandes áreas, acessíveis a partir dos separadores "Contas" e "Entidade". No separador "Contas" o utilizador tem acesso a operações diretamente relacionadas com as contas de gerência do Organismo/Entidade, o que dá a possibilidade de criar e editar as contas de gerência a entregar ao Tribunal de Contas, preenchendo a informação respeitante à regra contabilística que a entidade integra, mas também consultar o estado dos processos de conta de gerência, relativas às contas de gerência já entregues, por via electrónica ou não. É interessante ressaltar que a área a que o separador "Contas" conduz permite ao utilizador o acesso a contas de gerência em curso, que são contas que ainda não foram submetidas ao TC e a que só o utilizador tem acesso, a contas de gerência entregues e a contas de gerência sujeitas a alterações. (Consultado em TC de Portugal/Publicações, 2019)

A aplicação dá suporte para carregamento (upload) de ficheiros com uma dimensão máxima de 10 Mb e controlo do tipo, o nome do ficheiro tem de conter a extensão (exemplo: aaa.doc) e não pode conter no nome nenhum dos seguintes caracteres: / \ | : * ? "<>, e são admitidos os segujintes formatos: ficheiros Microsoft Office (extensões DOC, XLS, DOCX e XLSX); ficheiros Acrobat (extensão PDF); ficheiros de Texto (extensão TXT); ficheiros de Imagem (extensões JPG e TIF). (Consultado em TC de Portugal/Publicações, 2019)

Por fim, em consonância com o RGPD e tendo em conta a especificidade da atividade desenvolvida pelo DSTI, com o acompanhamento da Comissão de Informática, o EPD tem, entre outras funções: aconselhar, em caso de dúvida, sobre a admissibilidade da publicação, ou da disponibilização no sistema, de determinados dados pessoais constantes de relatórios de auditoria, sentenças, acórdãos ou despachos; promover a adoção de procedimentos internos de garantia do exercício dos direitos dos titulares de dados, designadamente no que diz respeito à tramitação de pedidos feitos por eles ao Tribunal de Contas; promover a avaliação do nível de segurança dos dados conservados pela DGTC, nomeadamente os referentes aos dados pessoais de juízes conselheiros e pessoal dos serviços de apoio, além do dever de identificar os dados que devam ser classificados como dados sensíveis, para poder avaliar e propor o ajustamento necessário do respectivo nível de segurança.

4.4 – Observações críticas, diretrizes e sugestões

É oportuno fazer algumas observações, aferidas a partir dos estudos realizados nos três Tribunais de Contas, uma vez que se percebe, com clareza, que os ditos Tribunais, mesmo o TC. de Portugal, o qual encontra-se num estágio mais avançado de adequação ao RGPD, ainda não dispõem de ferramentas precisas e eficazes que se ponham de acordo com os princípios da LGPD, notadamente com relação as regras de segurança e do sigilo de dados, bem como das boas práticas e de padrões técnicos que favoreçam aos titulares dos dados.

Algumas diretrizes hão de ser seguidas pelos provedores de conexão e de aplicações, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, a exemplo do estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades e de privilégios de acesso; da previsão de mecanismos de autenticação de acesso aos registros, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros; a criação de um inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pelo Tribunal e o arquivo acessado; o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes etc.

Para o alcance destas diretrizes pelos respectivos setores de TI dos Tribunais estudados, é importante que eles busquem alternativas disponíveis no amplo mercado de informática, o qual oferta três categorias de ferramentas, que se prestam a avaliar o que é preciso fazer para assegurar a conformidade, implementar medidas para atender aos requisitos e manter o funcionamento de seus sistemas ao longo do tempo de acordo com o RGPD e a LGPD, a saber: ferramentas de avaliação, ferramentas de implementação e ferramentas de manutenção[221].

Entre as ferramentas de avaliação, podem os Tribunais de Contas, através da área de TI, tomar como exemplo a ser desenvolvido pelos seus técnicos: a) "*Snow Software GDPR Risk Assessment*", que identifica mais de 23 mil versões de aplicativos que detêm ou transmitem dados pessoais, além de fornecer visibilidade sobre dispositivos, usuários e aplicativos, seja nas instalações, na nuvem ou no celular. Através da varredura passiva os agentes não precisam ser instalados nos nós de extremidade. Pode sinalizar os dispositivos que não possuem controles de segurança RGPD ou LGPD

[221] As informações e especificações sobre os dados técnicos de tais ferramentas podem ser facilmente buscadas nos respectivos links de acesso obtidos pelo direcionamento do cursor em suas denominações. Disponível em: https://cio.com.br/tendencias/14-principais-ferramentas-para-saber-se-voce-cumpre-os-requisitos-do-gdpr/. Acessado em: 10 de out. de 2020.

adequados para que a Entidade saiba onde seus dados estão, quem está usando e como está protegido; b) a "*The International Association of Privacy Professionals (IAPP) and TRUSTe GDPR Readiness Assessment",* que tem uma versão especial chamada "*TRUSTe Assessment Manager"*. Foi criada para membros do IAPP, e contém mais de 60 perguntas mapeadas para os principais requisitos do RGPD e produz uma análise de lacunas com as etapas recomendadas para remediação. A ferramenta de avaliação é baseada na nuvem e não exige um download de software. Integra-se com uma variedade de aplicações e ambientes de hospedagem existentes, incluindo Amazon Web Services e Alibaba Cloud; c) "DB DBN-6300", que é um dispositivo de segurança que utiliza inteligência artificial e análise de protocolo para dar visibilidade às atividades de infraestrutura do banco de dados. Ele também descobre intrinsecamente bases de dados contendo PII e aplicativos conectados e mapeia automaticamente como as informações estão sendo processadas. O DBN-6300 realiza varredura passiva em um ponto de acesso de rede em vez de usar a varredura ativa. Suporta sistemas de gerenciamento de banco de dados, incluindo Oracle Server, Microsoft SQL Server e SAP Sybase ASE. d) "*O Opus Global's Third-Party Compliance"* como solução de serviço (SaaS) move a avaliação para a cadeia de suprimentos, identificando terceiros com os quais os dados pessoais de seus clientes são compartilhados. Os questionários sobre controles de segurança de dados são enviados automaticamente para usuários externos. A ferramenta analisa as respostas para determinar se elas cumprem os requisitos RGPD, ou LGPD, e fornece recomendações para remediação. Isso permitiria, por exemplo, que os Tribunais de Contas documentasse completamente quem tem acesso a dados cobertos e como ele está protegido. Esta solução SaaS não requer hardware, software ou infraestrutura de TI. (CIO - cio.com.br/tendências/ferramentas, 2020)

No tocante às ferramentas de implementação, podem as Entidades buscar as seguintes soluções: a) A *"Secureprivacy.ai"* é uma solução automatizada de gerenciamento de consentimento para tornar os *sites* compatíveis com os requisitos das Leis de Proteção de Dados. Objetiva obter o consentimento informado dos usuários para coleta e uso de dados. Também permite que eles desapareçam. Uma vez instalado, o *script Secureprivacy.ai* fornece notificações detalhadas página a página para os requisitos adequados de *opt-in e opt-out*. As capturas de tela são salvas para documentar o consentimento do usuário e estão disponíveis através de um painel de controle. A solução é formatada para dispositivos *desktop e móveis* e inclui um *plugin* para usuários do *WordPress*. A documentação inclui o endereço IP do usuário e a localização e pode ser facilmente exportada para uso comercial e regulamentar; b) a "*Datum Information Value Management*" é uma edição especial de *software* de governança de informações que está pré-configurado com processos, regras, padrões, modelos e *frameworks* baseados no RGPD. Ele alinha os dados de uma organização com os requisitos

regulamentares, identificando os dados abrangidos pelas regras de privacidade da UE e os recursos e controles necessários. A ferramenta descobre os dados e como são usados, e mapeia o processo de governança da organização. Isso permite que os dados sejam usados e compartilhados com as partes interessadas em toda a organização dentro dos requisitos dos regulamentos de privacidade e a conformidade dos documentos para os reguladores; c) o "*SAS for Personal Data Protection"* cria um ambiente unificado com uma única interface de usuário para acessar e gerenciar dados. Permite que as organizações acessem, identifiquem, protejam e auditem dados pessoais para que possam cumprir os requisitos de proteção de dados e que os dados pessoais não devam apenas ser protegidos, mas removidos mediante solicitação. Esta combinação de software e serviços SAS permite que as organizações combinem tipos de dados de várias fontes, como Oracle, Apache e Hadoop, identificando dados pessoais em fontes estruturadas e não estruturadas. Os seus recursos de governança de dados aplicam políticas e protegem os dados por meio de máscara e criptografia baseadas em função que asseguram informações confidenciais enquanto estão em repouso e em uso; d) o "*Neupart Secure RGPD"* está baseado no sistema de gerenciamento de segurança seguro do ISMS da empresa. Os recursos adicionais projetados para que as empresas implementem e mantenham os processos GDPR incluem modelos, proteção de dados e ferramentas de avaliação de impacto, capacidade de notificação de violação de dados e análise de lacunas para rastrear seu status de conformidade atual. Ele também fornece um painel de instruções de proteção de dados para que os EDPs tenham uma visão única das principais áreas de conformidade; e) o *"Aircloak Insights*" permite que as organizações façam uso de dados protegidos, anonimizando-os para análise, a fim de que os resultados possam ser compartilhados sem restrições. A solução consiste em dois pedaços de software (o frontend web Air e o mecanismo de anonimização Cloak) que funcionam em dois recipientes do Docker para virtualização no Windows e no Linux. Funciona com os bancos de dados mais populares, incluindo um grande conjunto de bancos de dados SQL. (CIO - cio.com.br/tendências/ferramentas, 2020)

Por fim, há uma série de Ferramentas de manutenção que podem servir de suporte ao desenvolvimento particular dos Tribunais de Contas, tais como: a) "*BigID BigOps"* - uma ferramenta de varredura que usa *Machine Learning* para rastrear continuamente as alterações na PII[222] nos ambientes de produção e desenvolvimento, no data center ou na nuvem. O *Machine Learning* permite que o software compreenda dados pessoais conhecidos e seus contextos e, em seguida, descubra e catalogue

[222] De acordo com o Google , as informações de identificação pessoal (PII) podem incluir (mas não se limitam a) "informações como endereços de e-mail, números de celular pessoais e números de previdência social". Essa lista pode incluir números de cartão de crédito, endereços, nomes ou qualquer coisa que possa distinguir ou rastrear a identidade de um indivíduo. Resumindo: se um dado pode ser usado para distinguir a pessoa exata que fez aquela visita ou executou aquela ação, ele não pode ser passado para o Google Analytics. Embora todos nós tentemos cumprir as proteções de privacidade e várias leis, coletar PII por acidente é mais comum do que se possa imaginar. Disponível em: <https://www.upbuild.io/blog/pii-in-google-analytics/>. Acessado em: 05 de out. de 2020.

todos os dados pessoais nos compartimentos de dados. Integra-se com estruturas de automação, como a *Jenkins*, para monitorar as mudanças nos dados ao longo do ciclo de vida de desenvolvimento, ajudando a garantir que permaneça em conformidade com os requisitos do RGPD. Também ajuda com os requisitos para a resposta à violação de dados, permitindo que uma organização compare seus dados com a de um vazamento de dados roubados para determinar, em poucos minutos, se há violações ao RGPD; b) a "OneTrust", uma plataforma de software de gerenciamento de privacidade que automatiza tarefas para permitir a continuidade da conformidade com os requisitos do RGPD para os cookies do site e a manutenção de portais. A *OneTrust* realiza varreduras contínuas das páginas *Web* de uma organização para identificar e categorizar *cookies* e fornece um mecanismo transparente para obter os consentimentos necessários para cada *cookie*. Também pode ser usado para criar um portal para lidar com os pedidos dos usuários para gerenciar PII sob o RGPD. Pode acompanhar e documentar as solicitações dos usuários e a resposta da organização; c) a "*FileCloud*", conhecida como uma plataforma de compartilhamento e sincronização de arquivos empresariais. Oferece recursos para facilitar tarefas associadas a alguns requisitos do RGPD. As configurações de privacidade tornam mais fácil pedir aos usuários o consentimento ao acessar o conteúdo da nuvem. As ferramentas de administrador permitem a eliminação ou anonimização de PII para pedidos relacionados ao direito de serem esquecidos, ou para responder aos pedidos de quais PII uma empresa possui de um indivíduo. O *FileCloud* também aborda o requisito de portabilidade de dados com a capacidade de exportar em formatos padrão; d) a *"Loom Systems Sophie"* é uma ferramenta de operações de TI algorítmicas (AIOps), que usa inteligência artificial (AI) para analisar logs de máquina e dados não estruturados de forma a dar visibilidade imediata aos ambientes de TI. Possui um recurso "*Find my PII*" que automatiza a coleta de logs sensíveis. Isso facilita o cumprimento do direito de de ser esquecido, pois ele permite que se localize e se exclua rapidamente dados pessoais quando uma solicitação para remoção for recebida. (CIO-cio.com.br/tendências/ferramentas, 2020)

Ante o exposto, considerando os três Tribunais de Contas, é notório que cada organização deve envidar esforços para garantir a privacidade e a proteção dos dados pessoais e dos dados sensíveis que coletam, manipulam, processam e armazenam. A pergunta que vem à tona é simples, qual seja, - como anonimizar estes dados? A Sensitive Data Discovery, ou tecnologia de descoberta de dados sensíveis permite identificar quais são os dados, como os dados em diferentes fontes de dados estão relacionados, quais são esses relacionamentos e se existem dependências entre os elementos dos dados, independentemente se esses elementos estão em um único banco de dados ou em várias fontes de dados

heterogêneas[223].

Cabe às respectivas áreas de TI identificar os dados sensíveis e em seguida dispor de uma forma de protegê-los, entre elas, a anonimização. Podem, por exemplo, mascarar os dados (substituí-los por dados gerados e não sensíveis), criptografar os dados (de modo reversível ou irreversível) ou tokenizar os dados. A escolha de uma dessas opções dependerá dos requisitos de segurança e necessidades de desempenho. Abordemos em breve síntese cada uma delas.

O mascaramento de dados é, na maioria dos casos, uma opção altamente segura, porque substitui completamente os dados existentes, apesar de ter o custo de perder o acesso aos dados originais. O ponto é que seus dados mascarados podem ser gerados usando algoritmos de mascaramento para reter as propriedades relevantes dos dados originais, sendo ao mesmo tempo totalmente falsos. Por exemplo, o Tribunal de Contas pode precisar que os dados mascarados de um jurisdicionado, objeto de denúncia, mantenham a mesma estrutura que os dados que estão substituindo (por exemplo, um número de identificação, ou de acesso), para que se encaixem no mesmo intervalo ou tenham aproximadamente o mesmo valor. Em sua essência, o mascaramento de dados é útil quando não se importa com os dados em si, mas apenas com as propriedades mais importantes deles[224].

A criptografia, notadamente a do tipo irreversível, é a espinha dorsal da anonimização, e difere do mascaramento, ao permitir o acesso (altamente regulado) aos dados primários, um mal necessário para a maioria dos casos de uso. Por outro lado ao optar pela criptografia com preservação de formato (Format Preserving Encryption – FPE), que é reversível, os dados criptografados terão o mesmo formato que os dados originais. Ressalte-se, contudo, que esta última é significativamente menos segura, podendo como resultado, não estar em conformidade com alguns requisitos da legislação nacional e internacional de proteção de dados, pelo fato de poder ser revertida por um agente mal-intencionado.

O formato reversível pode ser útil para lidar com sistemas automatizados (automação de testes) que precisam de um formato de dados específico, mas não se importam com o conteúdo (a exemplo do número de um cartão de crédito, onde alguns usuários precisam ver os últimos quatro dígitos, mas outros não devem ver nada). A criptografia com preservação de formato é relativamente nova e muito específica, e compete com a tokenização. Uma outra opção é a criptografia homomórfica, que permite a computação em dados criptografados, gerando um resultado criptografado que, quando descriptografado, corresponde ao resultado das operações como se elas tivessem sido executadas em

[223] A LGPD e a anonimização de dados: mascaramento, criptografia e tokenização. Artigo inserto em leadcomm. Disponível em: https://leadcomm.com.br/2020/07/29/a-lgpd-e-a-anonimizacao-de-dados-mascaramento-criptografia-e-tokenizacao . Acessado em: 17 de out. 2020.

[224] Idem

dados não criptografados[225].

O Token, a seu turno, é um recurso de segurança, que gera um código identificador digital exclusivo, aleatório e temporário, para proteger dados sensíveis. A tokenização é caracterizada pelo fato de excluir a figura humana das interações e garantir a segurança de todos os dados "tokenizados". O token é frequentemente utilizado para autenticar transações online em instituições financeiras. Por exemplo, se o Tribunal de Contas precisar omitir legalmente o nome de um investigado, ao utilizar o token, o nome pode se converte no seguinte código - J!XZ&N25 e o número de identificação pode se tornar 3K3O?8/ após a tokenização. O efeito prático de tal conversão é a segurança em relação a um provável invasor não autorizado, a exemplo de um hacker, o qual, ao acessar um serviço de nuvem, tudo o que ele poderá ver serão símbolos sem sentido. Em geral, estes códigos são gerados aleatoriamente, sem nenhuma relação matemática com o campo de dados original, o que impossibilita a determinação do significado original de um dado sigiloso.

A tecnologia da informação proporciona diversas opções, e a decisão sobre qual método optar deve considerar as necessidades de cada Entidade, no caso, de cada Tribunal de Contas. Uma boa sugestão seria o uso de uma combinação dessas tecnologias, posto que ao contrário do mascaramento de dados, criptografia e tokenização são métodos de segurança criptográfica. A principal diferença entre eles reside no fato de que a tokenização preserva o formato, ao passo que a criptografia tradicional, não. Vale salientar, contudo, quando os dados são usados continuamente para objetivos de negócio, como testes e desenvolvimento, a criptografia ou a tokenização se tornam processos complicados. O usuário precisa usar uma chave para descriptografar o conjunto cifrado de dados ou usar o valor do token para recuperar os dados reais muitas vezes, para não arriscar que as informações sensíveis sejam acessadas indevidamente[226].

Ao fechar este tópico, não poderia deixar de registrar uma crítica em relação a lentidão com que os TCs analisados, mormente as respectivas áreas de TI, acompanham a evolução das ferramentas disponíveis a tornar mais efetiva e eficaz o tema proteção de dados em seus ambientes de trabalho. Com efeito, os estudos realizados nos Tribunais de Contas evidenciaram uma urgente necessidade de buscar ferramentas que se coadunem com as regras trazidas pelas legislações de proteção de dados, a exemplo das que foram explicitadas nas linhas precedentes. Neste sentido, estas Entidades Públicas não podem ficar à margem dos demais atores envolvidos (setor privado, titulares de dados, técnicos de informática

[225] A LGPD e a anonimização de dados: mascaramento, criptografia e tokenização. Artigo inserto em leadcomm. Disponível em: https://leadcomm.com.br/2020/07/29/a-lgpd-e-a-anonimizacao-de-dados-mascaramento-criptografia-e-tokenizacao . Acessado em: 17 de out. 2020.

[226] Idem

etc), carecendo urgentemente de uma mobilização na incrementação de seu "parque tecnológico", inclusive mediante a inclusão de recursos específicos em seus orçamentos. Acreditao que demandará um tempo razoável para o atingimento da desejável adequação ao RGPD e LGPD.

CONSIDERAÇÕES FINAIS

1. No introito deste trabalho, foi evidenciada a importância relevante da evolução tecnológica proporcionada pela Internet, reforçada pelo incremento das novas tecnologias de informação e comunicação – NTIC ao quotidiano das pessoas, do cidadão comum, bem como a consequência imediata provocada pela fácil acessibilidade do indivíduo as mais variadas ferramentas e dispositivos eletrónicos disponíveis, qual seja a exposição a público de sua vida privada, de seus dados pessoais.

2. Este "bum" tecnológico, por outro lado, exigiu a ação das autoridades públicas, notadamente das que desempenham a atividade legislativa, no sentido de resguardar e de proteger a privacidade afetada pela interferência virtual alheia por meio de instrumentos jurídicos apropriados e legítimos, consubstanciados em atos normativos primários, vale dizer, mediante a edição de leis protetivas dos dados pessoais de pessoas singulares, a exemplo do RGPD Europeu e da LGPD brasileira.

3. A questão da regulamentação do acesso e o consequente uso de dados extrapolou a esfera privada, e necessário se fez obter o equilíbrio desejado entre a proteção de nossa privacidade e a permissão para explorar os dados gerados, seja por uma empresa, seja por uma Entidade Pública. É um direito do titular a ser respeitado, posto que, conforme assevera Teresa Moreira, "ninguém deve ser pressionado para dar a sua *password* de acesso às redes sociais ou ter de fornecer os dados dos seus amigos *online*"[227], o que alcança inclusive as Entidades Públicas, tanto na condição de empregadores de seus funcionários públicos quanto no desempenho de atividades que requeiram a recolha, produção, utilização, armazenamento, enfim, operações de tratamento de dados.

4. É no contexto destas atividades suprareferenciadas que se desenvolveu o tema deste trabalho, no qual se buscou analisar o nível de implantação do RGPD Europeu e da LGPD do Brasil, particularmente no âmbito de um dos "braços" da Administração Pública, que tem a sua competência definida nas respectivas Constituições Republicanas – os Tribunais de Contas. Como forma de endereçar a análise, a pesquisa limitou-se, a um comparativo do grau de adequação das normas internas do Tribunal de Contas de Portugal, do Tribunal de Contas do Estado Rio Grande do Norte e do Tribunal de Contas do Estado da Paraíba às regras das referidas normas protetivas de dados pessoais.

[227] MOREIRA, Teresa Coelho. "*A Privacidade dos trabalhadores e as Novas Tecnologias de Informação e Comunicação: Contributo para um Estudo dos Limites do Poder de Controlo Electrónico do Empregador, Coimbra, Almedina, 2010, p.100.*

5. O primeiro desafio desta dissertação consistiu em contextualizar a temática proposta, tendo em conta dois pontos a serem observados. O primeiro referiu-se à diferença existente entre o estágio de implantação do RGPD nos Organismos Europeus e a desejada e porvir adequação da LGPD pelas Instituições Públicas e Privadas do Brasil, restando inequívoco que o diploma normativo Europeu coloca-se muito à frente e em fase de consolidação, servindo inclusive de referência para o estudo destinado à implementação do similar normativo brasileiro. Verificou-se que as discussões levada a cabo no âmbito de doutrinadores e legisladores no Brasil, a exemplo do ocorrido na comissão legislativa especial destinada a proferir parecer ao projeto de Lei nº 4060/2012, que dispôs sobre o tratamento e proteção de dados pessoais, culminaram pela publicação da LGPD, a Lei nº 13.709/2018, posteriormente alterada pela Lei nº 13.853/2019, a qual criou a Autoridade Nacional de Proteção de Dados do Brasil.

6. O segundo ponto trouxe à baila a preocupação reinante na doutrina do possível conflito que poderia vir a existir quando da aplicação do RGPD e da LGPD ante às disposições das legislações que disciplinam e garantem ao indivíduo o acesso à informação, que foi tratado no item 2.4 deste trabalho. Quanto a este aspecto, vimos que as regras de ambas as legislações complementam-se e que devem ser preservados sobretudo os direitos fundamentais garantidos pelas respectivas Constituições Republicanas. Ademais, ao abordarmos os principais conceitos trazidos pelo RGPD e LGPD, relacionados à proteção de dados e a serem incorporados ao ambiente de trabalho e à mentalidade de servidores públicos, funcionários, contratados etc, pode-se aferir o quão específicas e técnicas são as leis protetivas de dados pessoais quando comparadas as respectivas legislações portuguesa e brasileira que disciplinam o acesso à informação.

7. Com a contextualização do tema e o conhecimento dos novos conceitos incorporados ao quotidiano das atividades dos destinatários do RGPD e da LGPD, o passo seguinte foi a definição do conteúdo, do âmbito material a ser considerado na aplicação destes diplomas normativos pelos Tribunais de Contas. Ou seja, uma análise baseada nas disposições legais do RGPD com vistas a delimitar o papel desses atores e o consequente emprego da *accountability* como meio de fiscalização e controle da tutela da privacidade e proteção de dados a serem cumpridos no desempenho das atribuições daquelas Entidades de Controle Externo. Há, portanto, um conjunto de regras e obrigações que deverão necessariamente serem levadas em conta, notadamente as que dizem respeito aos direitos dos titulares de dados, agora elevados ao nível de direito fundamental, além de princípios a serem aplicados quando do tratamento dos dados pessoais, independentemente da nacionalidade ou do local de residência dessas pessoas, nos termos previstos na CDFUE e no TFUE. Isto implica a adoção de soluções técnicas que permitam dar respostas adequadas e satisfatórias às solicitações formulads pelos titulares dos dados, sob pena de descumprimento de suas normas e consequente cominação das penalidades previstas em lei.

8. Na sequência do trabalho, mereceu uma particular atenção um estudo sobre as regras aplicáveis ao tratamento de dados pessoais por instituições, órgãos comunitários, organismos ou agências da União, o que demandou a análise de alguns dispositivos do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, notadamente o Capítulo IV, e a sua conexão com o RGPD. Vimos que os dois conjuntos de disposições devem ser interpretados de forma homogênea, observado o critério de que *lex specialis derogat legi generali,* relativamente ao tratamento de dados pessoais operacionais. Ademais, as disposições específicas hão de guardar coeréncia com os princípios subjacentes ao capítulo relativo ao tratamento de dados pessoais operacionais, e também com as disposições regulamento relativas ao controlo independente, às vias de recurso, à responsabilidade e às sanções. Em suma, como assevera Norberto Bobbio, "*a situação de normas incompatíveis entre si é uma das dificuldades frente as quais se encontram os juristas de todos os tempos, tendo esta situação uma denominação própria: antinomia. Assim, em considerando o ordenamento jurídico uma unidade sistêmica, o Direito não tolera antinomias."*[228] Superada esta questão, observou-se que em ambas as normas, além de outras convergências, há uma considerada fundamental, por se tratar de um elemento responsável por assegurar que as disposições do regulamento sejam aplicadas por cada instituição ou órgão público, a saber, o *Data Protection Officer*, ou encarregado de proteção de dados. Neste desidério, vimos que uma das primeiras iniciativas do Tribunal de Contas de Portugal foi a designação de seu encarregado, nos moldes propostos pelo regulamento.

9. A compreensão dos aspectos atinentes às Instituições e Órgãos Públicos do RGPD embasaram as regras específicas do Poder Público do Brasil aplicáveis ao tratamento de dados pessoais, para o qual a LGPD dedicou nove artigos em seu capítulo IV, estabelecendo regras e responsabilidades ao tempo em que procurou harmonizar as disposições relativas ao acesso à informação nas mãos da administração pública com a proteção de dados pessoais dos cidadãos. Numa análise comparativa, vimos que há uma diferença nos critérios de tratamento de dados pelas Entidades Públicas no Brasil, posto que em se tratando de empresas públicas e sociedades de economia mista que atuam em regime de concorrência, aplica-se a elas o mesmo tratamento dispensado pela LGPD às pessoas jurídicas de direito privado, ao passo que se estiverem operacionalizando políticas públicas, o tratamento a ser dado será o mesmo aplicado aos demais órgãos e às entidades do Poder Público. Aos Tribunais de Contas do Brasil, aplicam-se, portanto, as regras contidas no Capítulo IV da LGPD.

10. Uma vez delineadas as regras essenciais à compreensão do tema em curso, o trabalho enveredou no campo de pesquisa junto ao TCE/RN, TCE/PB e ao TC de Portugal, objetivando colher elementos e material que fornecessem subsídios para apresentar o nível de adequação de suas normas

[228] BOBBIO, Norberto. *Teoria Geral do Direito*. Martins Fontes, 2007. p. 219 – 259.

internas e atribuições da área de Tecnologia da Informação com os requisitos impostos pelo RGPD e pela LGPD. Não se constituiu em tarefa elementar a conjugação das estruturas normativas institucionais com as normas de proteção de dados pessoais e, por isto, dedicou-se o capítulo III a estabelecer o nível de interação existente entre as lesgislações *interna corporis* do Tribunal de Contas de Portugal e o RGPD da União Europeia, e dos Tribunais de Contas do Brasil em relação a LGPD.

11. Como explicitado no preâmbulo do citado capítulo, partiu-se de um referencial teórico buscado em alguns diplomas normativos que precederam a elaboração das respectivas legislações sobre proteção de dados pessoais. Com base no dito referencial, elaborou-se um questionário dirigido a alguns funcionários dos TC's, notadamente os dirigentes de departamentos, a fim de se obter informações que permitissem deles aferir o grau de envolvimento, interesse, participação e importância das regras relativas à proteção de dados pessoais para a escorreita atuação destas Entidades, como também, e principalmente, para atestar o conhecimento de todos acerca de uma Legislação de Proteção de Dados.

12. A análise dos resultados revelou que as respostas obtidas não apresentaram uma avaliação positiva na relação entre funcionários e o conhecimento da LGPD, o que pode ser confirmado ao confrontar as normas internas de cada um dos TC's do Brasil, eis que os dois principais atos normativos, a Lei Orgânica e o Regimento Interno, praticamente não tratam de modo explícito em seus textos acerca da Proteção de Dados Pessoais, sejam eles os dados relativos aos informes dos jurisdicionados ou mesmo os relativos aos seus servidores. Isto demonstra porque apenas um percentual ínfimo de funcionários sabe quais os tipos de dados e informações são tratados pela área de TI dos TC's.

13. Tal constatação exige uma mudança de paradigma a ser trabalhada e incluída nos respectivos Planejamentos Estratégicos da Tecnologia da Informação que, a seu turno, deverá contemplar, entre suas ações, a de conciliar as atribuições específicas da área de TI e adequá-las aos requisitos e princípios exigidos pela LGPD. Trata-se de um desafio a ser enfrentado pela área de informática, não apenas no aspecto técnico propriamente dito, mas também na disseminação interna dos novos conteúdos introduzidos pela LGPD, e o consequente disciplinamento das responsabilidades a serem assumidas pelo material humano, seja este funcionários ou terceirizados, observadas as disposições legais de contratação de pessoal para terceirização dos serviços de informática.

14. Ao confrontar a disciplina normativa dos TC's do Brasil com as existentes no TC. de Portugal, foi constatado e confirmado que este último alçou a sua área de Tecnologia da Informação a uma posição de destaque em sua organização e estrutura, tamanha a importância das atividades ali desenvolvidas, o que, de certa forma, tem tornado mais fácil a adequação aos requisitos exigidos pelo RGPD. Com efeito, o TC. de Portugal, ante a iminência da entrada em vigor do RGPD, antecipou-se e dedicou-se ao estudo de suas regras e as conclusões daí decorrentes resultou na publicação de um ato

normativo interno em cujo conteúdo estão registradas as medidas adotadas para materializar a aplicação do RGPD no Tribunal de Contas.

15. A par disso, o Planeamento Estratégico vigente enfatiza entre os seus objetivos a preocupação sistemática com a flexibilidade, encarada como capacidade de ajustamento às mudanças rápidas e imprevistas próprias de uma realidade globalizada, interligada e digitalizada, bem como estabelece entre os eixos prioritários de ação a promoção da segurança da informação, a habilitação em meios e competências digitais, a desmaterialização e automação de processos e procedimentos, com recurso à inteligência artificial, na fiscalização prévia, nas várias formas de fiscalização concomitante e sucessiva e nos julgamentos, bem como no controlo dos dados e informações em nível interno. É irrefutável que, para o alcance da concretização destes eixos, necessário se faz um relevante investimento na modernização e reorganização da sua estrutura tecnológica, na qualificação de seus técnicos e na disseminação de conhecimentos com vistas a à preparação para a sociedade digital.

16. O último capítulo deste trabalho abordou o que os sistemas de acompanhamento de gestão dos TC's dispõem em termos de ferramentas para tornar viável a efetiva e adequada proteção de dados pessoais ao realizar as funções constitucionais no exercício de suas competências. Vimos que, conquanto os TC's possuam sistemas de TI distintos (SIAI Fiscal, no TCE/RN; SAGRES, no TCE/PB; e GENT, no TC. de Portugal), há uma convergência no tocante ao zelo pelo tratamento de dados e informações, tanto as alimentadas pelos jurisdicionados quanto aquelas referentes aos seus funcionários. Não se pode olvidar, contudo, que os requisitos exigidos pelo RGPD e pela LGPD requer dos funcionários do setor de TI uma revisão detalhada dos sistemas já em operação para, num segundo momento, adequar as ferramentas disponíveis as regras de proteção de dados dos titulares envolvidos que, no caso dos TC's, não se limitam apenas aos ocupantes de cargos em sua estrutura interna, senão também e, principalmente, aos dados alimentados pelos titulares das diversas esferas de poder (Estados e Municípios).

17. No estágio atual, como foi observado, os TC's do Brasil ainda não estabeleceram formalmente os agentes de tratamento de dados à luz da LGPD. O procedimento de acesso de usuários externos aos portais dos TC's acontece por meio de sistemas próprios, sendo exigido o prévio cadastramento e posterior validação. A autorização ao acesso de dados internamente pelos funcionários e a definição de perfis cabe às chefias imediatas; externamente, cada jurisdicionado possui um usuário gerenciador que realiza a gestão dos seus próprios usuários com os respectivos controles de acesso, e os dados são transmitidos por meio dos sistemas disponibilizados aos jurisdicionados via Internet.

18. Em relação ao TC. de Portugal, já é possível identificar a influência do RGPD no *modus operandi* de seu sistema, o que se confirma pela adoção de medidas fundamentais entre as quais estão: a

adequação da publicitação do conteúdo dos atos do Tribunal ao princípio da minimização dos dados; a designação de um EPD e a definição do respectivo estatuto, com o detalhamento de sua missão e funções em alinhamento com o RGPD. Desta forma, o EPD assume, no âmbito do Tribunal, todas as operações de tratamento realizadas pelo responsável pelo tratamento ou pelo subcontratante, mesmo aquelas que não digam respeito ao desempenho de funções públicas ou oficiais, *e.g* da gestão de base de dados de trabalhadores ou de fornecedores. Como foi explicitado, na caracterização do conteúdo funcional do EPD, o TC. de Portugal fundamentou-se nas orientações sobre os EPD do Grupo de trabalho do Artigo 29° para a Proteção de Dados, da Diretiva 95/46/CE (GT29). Vale salientar que o Tribunal está em permanente estudo promovendo os ajustes necessários a conformação com o RGPD.

19. Feitas estas considerações, e considerando que os TC's do Brasil, bem como as demais Entidades e Órgãos que compõem a Administração Pública estão delineando um padrão que assegure a proteção de dados de acordo com os requisitos da LGPD, não poderia deixar de trazer uma contribuição para o aperfeiçoamento da aplicação desta legislação, razão pela qual apresento nas linhas que se seguem algumas etapas preparatórias a serem observadas, fruto da pesquisa bibliográfica realizada ao longo do desenvolvimento desta dissertação.

20. As etapas estão baseadas na metodologia de preparação para aplicação da LGPD elaborada pela Comissão Nacional de Informação e Libertação da França – CNIL[229] e contempla as seguintes fases: I) a designação de um EPD; II) o mapeamento dos tratamentos de dados pessoais existentes; III) o estabelecimento de prioridades das ações a empreender; IV) a gestão de riscos; V) organização dos procedimentos internos; VI) a segurança e a classificação da informação; e VII) a documentação da conformidade ao LGPD. Sem pretensão de esgotar as características a elas inerentes, estas etapas podem ser assim sintetizadas:

20.1 Tanto o RGPD quanto a LGPD estabelecem a nomeação ou designação de um EPD. É uma medida de fundamental importância devido as atribuições a ele conferidas, entre as quais a de se reportar ao Controlador, ou seja, o próprio Tibunal de Contas. Deve ser designado com base nas suas qualidades profissionais, em especial nos conhecimentos especializados no domínio do direito e das práticas de proteção de dados. Ao designado para esta função, que pode ser pessoa natural ou pessoa jurídica, deve ser assegurado o envolvimento de forma adequada e em tempo útil, em todas as questões relacionadas com a proteção de dados pessoais. Desta forma, encarregado será responsável por atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD; deverá ter acesso

[229] A CNIL é a Autoridade de Proteção de Dados da França e trata-se de um órgão regulador administrativo independente cuja missão é garantir que a lei de privacidade de dados seja aplicada à coleta, armazenamento e uso de dados pessoais. Disponível em: <www.cnil.fr/en/home>. Acessado em: 15 de jul. de 2020.

direto à alta administração, autonomia, estabilidade e navegabilidade em toda a instituição; responderá pelo tratamento dos dados pessoais conforme as informações fornecidas pelo controlador; prestará orientação aos demais funcionários e contratados acerca das práticas de tratamento de dados; coordenará políticas e práticas de privacidade, treinamentos e outras atribuições correlatas.

20.2 Com o objetivo de aferir o impacto da legislação de proteção de dados, necessário se faz mapear: os diferentes tratamentos de dados pessoais; as categorias de dados pessoais tratados; os objetivos das operações de tratamento de dados; os colaboradores que tratam os dados; os fluxos que existem, indicando a origem e o destino dos dados. Para isso, é importante identificar quem trata os dados; qual é a categoria de dados tratados; com que finalidade os dados são tratados; onde são armazenados os dados; por quanto tempo cada categoria de dados é conservada; as medidas de segurança adotadas a fim de minimizar os riscos de acesso não autorizados.

20.3 Uma vez mapeados os dados, deve-se estabelecer prioridades nas ações a empreender, o que implica em: assegurar-se de que apenas os dados estritamente necessários à prossecução dos seus objetivos são recolhidos e tratados; identificar a base jurídica em que se fundamenta o tratamento (por exemplo, o contrato, consentimento do titular dos dados, interesse legítimo, obrigação legal); prever as modalidades em que os titulares dos dados exercerão os seus direitos; verificar as medidas de segurança existentes; estar atento ao tratamento de dados pessoais sensíveis.

20.4 Gerir os riscos significa que, uma vez identificados tratamentos de dados com possibilidade de produzir riscos elevados para os direitos e liberdades dos titulares dos dados, deve ser realizada uma avaliação de impacto sobre a proteção de dados (AIPD) para cada tratamento. De acordo com o Manual de Gestão de Riscos do TCU[230], um dos princípios aplicáveis à Gestão de Riscos é a sua aplicação de forma contínua e integrada aos processos de trabalho de uma instituição. Uma vez mapeados, esses processos de trabalho produzem informações que irão dar suporte as seguintes etapas: estabelecimento do contexto; identificação dos riscos; análise dos riscos; avaliação do riscos; tratamento dos riscos; comunicação e consulta com partes interessadas; monitoramento; e melhoria contínua.

20.5 A organização dos procedimentos internos visam garantir a proteção permanente dos dados e implicam na adoção do *"privacy by design"*, ou seja, a proteção dos dados desde a sua concepção; a elaboração de umplano de formação e de comunicação para os colaboradores; o tratamento das reclamações e dos pedidos dos titulares dos dados no exercício de seus direitos; bem como a antecipação das violações de dados pessoais.

20.6 Como foi delineado alhures, à luz da LGPD e também do RGPD, a fim de garantir que

[230] BRASIL, Tribunal de Contas da União. *Manual de Gestão de Riscos do TCU*. Brasília, DF: TCU, 2018. Disponível em: <https://drive.google.com/file/d/1YEHkCaLgyfg3qxW6tJxOxER-Q1YTte8d/view> . p. 18. Acesso em: 27 de jul. de 2020.

os dados pessoais sejam processados de forma segura, devem ser implementadas medidas técnicas e administrativas adequadas pelas Instituições. Para o alcance destas medidas, a doutrina destaca entre outros, quatro princípios básicos aplicáveis à Segurança da Informação231, a serem observados: a autenticidade, a integridade, a confidencialidade e a disponibilidade. Tais princípios são de fundamental importância para as atividades finalísticas desenvolvidas pelos Tribunais de Contas, senão vejamos:

20.6.1 A autenticidade garante a veracidade da fonte das informações. Por meio da dela é possível confirmar a identidade da pessoa ou entidade que presta as informações;

20.6.2 A integridade consiste na fidedignidade de informações. Sinaliza a conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados efetuados. Sinaliza, ainda, a conformidade dos dados transmitidos pelo emissor comos recebidos pelo destinatário. A manutenção da integridade pressupõe a garantia de não violação dos dados com intuito de alteração, gravação ou exclusão, seja ela acidental ou proposital;

20.6.3 A confidencialidade consiste na garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação. Sua manutenção pressupõe assegurar que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal procedimento;

20.6.4 Por fim, a disponibilidade implica na garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores da informação e a área de informática. Manter a disponibilidade de informações pressupõe garantir a prestação contínua do serviço, sem interrupções no fornecimento de informações para quem é de direito.

20.7 A documentação da conformidade ao LGPD implica em reunir a documentação que relativa ao tratamento de dados pessoais que contenha: o registro dos tratamentos feitos pelos responsáveis; as AIPD relativas aos dados suscetíveis de gerar riscos elevados para os direitos e liberdades dos titulares dos dados; além do enquadramento das transferências ou do compartilhamento de dados com terceiros.

21. A compreensão do processo de aplicação da lei de proteção de dados pessoais

---

[231] BRASIL, Tribunal de Contas da União. *Boas práticas em segurança da informação*. 4. ed. Brasília, DF: TCU, 2018. Disponível em: <https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A24D6E86A4014D72AC823F5491&inline=1>. p. 9-10. Acesso em: 23 de jul. de 2020.

no âmbito dos Tribunais de Contas constitui-se, portanto, em primícia necessária à implementação das regras ali contidas, o que importa em permanente trabalho a ser desenvolvido pelas diversas áreas e atores envolvidos. Conclama a participação da alta administração, mediante a inclusão desta ação entre os objetivos do planejamento estratégico, como forma de assegurar os recursos necessários à área da tecnologia da informação para o desenvolvimento de ferramentas e a constante atualização dos sistemas de TI.

22. É inquestionável que a busca pela adequação aos aspectos inovadores da LGPD, similarmente ao ocorrido com o RGPD, comporta investimentos diversificados que vão desde as questões técnicas – de desenvolvimento de ferramentas, aplicações, de segurança da informação, gestão de processos, gestão de riscos, mapeamento de bases, fluxos e procedimentos, até a qualificação dos agentes de tratamento de dados, do treinamento e capacitação de pessoal.

23. No caso dos TC's do Brasil, ante os avanços alcançados nos últimos anos em termos de transparência, controle social e participação popular, proporcionados pelo amplo acesso e disseminação de informações, o caminho a ser percorrido para conformação de suas normas internas com as disposições da LGPD deverá ter em conta a existência de outros diplomas normativos, a exemplo da LAI, cuja ementa, como vimos, dá cumprimento a preceito estabelecido na Constituição Federal. Requer, portanto, uma aplicação de forma integrada das leis, conciliando-as, de tal modo que sejam respeitados os direitos assegurados aos titulares dos dados.

24. Com relação ao TC. de Portugal, como vimos ao longo deste trabalho, pode-se dizer que o RGPD trouxe um facilitador ao processo de adequação de suas normas internas, posto que o Regulamento, ao uniformizar as regras de proteção de dados, explicita em seu texto que a competência das autoridades de controlo não abrange o tratamento de dados pessoais efetuado pelos tribunais no exercício de sua função jurisdicional. Com isto, restou assegurada a independência do poder judicial no exercício de sua função jurisdicional, nomeadamente a tomada de decisões.

25. Por fim, sob uma perspectiva acadêmica e profissional, creio que este trabalho vem a ampliar as discussões a respeito da aplicação do RGPD e da LGPD tanto em relação aos TC's que foram objeto da pesquisa, quanto aos demais Tribunais de Contas não contemplados, bem como as demais Entidades do Poder Público. É cediço, contudo, que o presente estudo encontrou limitações, próprias ao desafio de enfrentar um tema que é tão atual e, ao mesmo tempo, inovador para os seus destinatários. Existem muitos pontos obscuros e

que deverão pautar as discussões durante e também após a implementação das regras de conformidade no setor público. Ademais, necessário se faz a adoção de uma postura mais proativa, porquanto tal como o que tem ocorrido nos países europeus, em virtude da implantação do RGPD, a administração pública tem andado a passos lentos quando se trata de adequação à LGPD. É o que se espera das autoridades e poderes constituídos.

REFERÊNCIAS BIBLIOGRÁFICAS

ALEXANDRINO, Marcelo; PAULO, Vicente. *Direito administrativo descomplicado*.- 24. ed. Rio de Janeiro: Forense; São Paulo, 2107.

ALMEIDA, José Luís Pinto. *Tribunal de Contas: Controlo Financeiro, Fiscalização Prévia, Concomitante e Sucessiva*. In Revista de Finanças Pública e Direito Fiscal. Ano 1, número 3 – Almedina, 2008.

ANDRADE, José Carlos Vieira de. *Os Direitos Fundamentais na Constituição Portuguesa de 1976*, Coimbra: Almedina, 2012.

ANDRADE, Francisco C.P.; COSTA, Angelo; NOVAIS, Paulo. *Privacidade e Proteção de Dados nos cuidados de saúde de idosos*. UMINHO. Artigo em ata de conferência. p. 12. 2011. Disponível em: https://repositorium.sdum.uminho.pt/ Acessado em: 01 de julho de 2020.

ANDRADE F., Neves J., NOVAIS P., MACHADO J., ABELHA A., *Legal Security and Credibility in Agent Based Virtual Enterprises*, in Collaborative Networks and Their Breeding Environments, CAMARINHA-MATOS L. Afsarmanesh H., ORTIZ A., (Eds), Springer-Verlag, ISBN 0-387-28259-9, pp 501-512, (IFIP TC5 WG 5.5 - 6th Working Conference on Virtual Enterprises (PRO-VE'05),Valencia, Spain), 2005. Disponível em: http://dx.doi.org/10.1007/0-387-29360-4_53.

ANDRADE, Francisco. *Comunicações Eletrónicas e Direitos Humanos: O perigo do "Homo Conectus."* Disponível em: https://repositorium.sdum.uminho.pt/

BANDEIRA DE MELLO, Celso Antônio. *Curso de direito administrativo*. 19. ed. São Paulo. Malheiros. p.51, 2005.

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

BIONI, Bruno Ricardo. *O papel do Data Protection Officer*. Jota. Disponível em: https://brunobioni.com.br/blog/2017/12/04/o-papel-do-data-protection-officer/. Acessado em: 04 de mar. de 2020.

BIONI, Bruno Ricardo. *Proteção de dados pessoais*. *A função e os limites do consentimento*. Rio de Janeiro: Forense, 2019.

BOBBIO, Norberto. *Teoria Geral do Direito*. São Paulo: Editora Martins. Martins Fontes, 2007.

BRASIL. SERPRO. *Data lake e big data tendencia no uso de dados públicos*. Brasília, 2017. Disponível em: <www.serpro.gov.br/menu/noticias>. Acessado em: 2 de jun. de 2020.

BRASIL, Tribunal de Contas da União. *Boas práticas em segurança da informação*. 4. ed. Brasília, DF: TCU, 2018. Disponível em:

<https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A24D6E86A4014D72AC823F5491&inline=1>. p. 9-10. Acessado em: 23 de jul. de 2020.

BUCKLAND, Michael. *Information and information systems*. Westport, CT: Praeger, p. 45. 1991.

CALVÃO, Filipa. *O modelo de supervisão de tratamentos de dados pessoais na União Europeia: da atual diretiva ao futuro regulamento*. In: Revista Forum de Proteção de Dados, n.º 1, julho, 2015.

CANOTILHO, J. J. Gomes; MOREIRA, Vital. *Constituição da República Portuguesa Anotada*, v. I. Coimbra: Coimbra Editora, 2014.

CANOTILHO, Mariana (Coord.). *Carta dos Direitos Fundamentais da União Europeia Comentada*. Coimbra: Almedina, 2013.

CARNEIRO, Davide Rua e NOVAIS, Paulo. *Behavioral Biometrics and Ambient Intelligence: New Opportunities for Context-Aware Applications*. State of the Art, in AI - Applied to Ambient Intelligence, 2017.

CARNEIRO J., SARAIVA P., MARTINHO D., Marreiros G., NOVAIS P., *Representing decision-makers using styles of behavior: An approach designed for group decision support systems, Cognitive Systems Research*, Elsevier, ISSN: 1389-0417, Vol. 47, pp 109-132, 2018. Disponível em: https://doi.org/10.1016/j.cogsys.2017.09.002.

CARNEIRO D., NOVAIS P., NEVES J., *Conflict Resolution and its Context. From the Analysis of Behavioural Patterns to Efficient Decision-Making*, Springer-Verlag, 279 pages, ISBN: 978-3-319-06238-9, 2014. Disponível em: http://dx.doi.org/10.1007/978-3-319-06239-6.

CARNEIRO D., NOVAIS P., ANDRADE F., ZELEZNIKOW J., Neves J., *The Legal Precedent in Online Dispute Resolution*, in Legal Knowledge and Information Systems, ed. Guido Governatori (proceedings of the Jurix 2009 - the 22nd International Conference on Legal Knowledge and Information Systems, Rotterdam, The Netherlands), IOS press, ISBN 978-1-60750-082-7, pp 47--52, 2009.

CASTRO, Catarina Sarmento e – *Direito da Informática, privacidade e Dados Pessoais,* Coimbra: Almedina, SA, 2005.

CAVALCANTI, Themistóclis Brandão. *Teoria dos atos administrativos*. São Paulo: ed. RT. p. 67, 1973.

CAVOUKIAN, Ann. *Privacy by Design: The 7 Foundational Principles*. August, 2009. Disponível em: <https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/ >.

COSTA, Thiago; RAMALHO, David. "*LEGAL ALERT - Nova Orientação do Grupo de Trabalho do 29.º relativa a Avaliações de Impacto sobre a Proteção de Dados*". Disponível em: < https://www.mlgts.pt/xms/files/v1/Publicacoes>

COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais comentada.* 2.ed.rev. atual. e ampl.- São Paulo: Thomson Reuters . Brasil, 2019.

CUEVA, Ricardo Villas Bôas. *A insuficiente proteção de dados pessoais no Brasil.* Revista de Direito Civil C ontemporâneo, São Paulo, v. 13, ano 4. p. 66, 2017.

DI PIETRO, Maria Sylvia Zanella. *Direito Administrativo* - 29.ed. Rev., atual. e ampl. - Rio de Janeiro: Forense, 2016.

ELMASRI, Ramez; NAVATHE, Shamkant B. *Sistemas de banco de dados*. 7. ed. São Paulo: Addison Wesley, p. 37-43. 2018.

FAZENDEIRO, Ana. *Regulamento Geral sobre Proteção de Dados*. 3 ed. – (textos da lei). Coimbra. ALMEDINA. Setembro, 2018.

FRAZÃO, Ana de Oliveira; MEDEIROS, Ana Rafaela Martinez. *Desafios para a efetividade dos programas de compliance.* In: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. *Compliance: perspectivas e desafios dos programas de conformidade.* Belo Horizonte: Fórum, 2018.

FRAZÃO, Ana de Oliveira; *Plataformas digitais e os desafios para a regulação jurídica.*. In: PARENTONI, Leonardo; GONTIJO, Bruno Miranda; LIMA, Henrique Cunha Souza (Orgs.). *Direito, tecnologia e inovação.* Belo Horizonte: D'Plácido, v. I, 2018.

JANEIRO, D. B. *La protección de datos de carácter personal en el derecho comunitario*. Anuario da Facultade de Dereito da Universidade da Coruña, p. 133-156, 2002.

JAY, Rosemary; MALCOLM, William; PARRY, Ellis; ET AL. *Guide to General Data Protection Regulation.* [s.I.]: Sweet & Maxwell, 2017.

LEONARDI, Marcel. *Tutela e Privacidade na Internet.* São Paulo: Saraiva, 2012.

MARAS, Marie-Helen. *Internet of things: security and privacy implications*. Internacional Data Privacy Law, v. 5, n. 2, 2015.

MATOS, Sara Margarida da Silva. *Biometria e privacidade: desafios bioéticos na cooperação policial e judicial na União Europeia*. In A. F. Sol & S. S. Gouveia (Eds), Bioética no Século XXI (pp. 255–286). Charleston: CreateSpace Independent Publishing, 2018.

MATTEI, Ugo. *Efficiency in legal transplants: An essay in Comparative Law and Economics, Intyernational Review of Law and Economics*. v. 14, p. 3-19, 1994.

MAURO, Roberta. *Em Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro* [livro eletrônico] / Ana Frazão, Gustavo Tepedino, Milena Donato Oliva coordenação. -- 1. ed. -- São Paulo : Thomson Reuters Brasil. Parte I, Cap. 5. p. 5, 2019.

MELO, Antônio. *Estudo sobre a avaliação de impacto sobre a proteção de dados*. Disponível em: <www.tcontas.pt/geral>. Acessado em: 22 de fev. de 2020.

MENDES, Laura Schertel; DONEDA, Danilo. *Marco jurídico para a cidadania digital: uma análise do Projeto de Lei 5.276/2016. Revista de Direito Civil Contemporâneo*, São Paulo, v. 9, ano 3, p. 35-48, out.-dez. 2016.

MIRANDA, Jorge; MEDEIROS, Rui. *Constituição Portuguesa Anotada*. 2.ed., Coimbra Editora, 2010.

MONTE, Mário Ferreira; BRANDÃO, Paulo de Tarso. *Direitos Humanos e a sua efetivação na Era da Transnacionalidade* – Debate Luso-Brasileiro, Juruá Editora, 2012.

MOREIRA, Teresa Coelho. "*A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação: contributo para um estudo dos limites do controlo eletrónico do empregador".*Almedina, 2010.

MOREIRA, Teresa Alexandra Coelho. *A proteção de dados pessoais dos trabalhadores e a utilização de tecnologias de identificação por radiofrequência*. In Memórias do XVI Congresso Ibero Americano de Derecho e Informática, Quito, 2012.

MOREIRA, Teresa Alexandra Coelho. "*Os dados pessoais dos trabalhadores e o contrato de teletrabalho subordinado*", in Fodertics 4.0 – *Estudios sobre Nuevas Tecnologías y Justicia,* (coord. Federico Bueno de Mata), Editorial Comares, Espanha, 2016.

MOREIRA, Teresa Alexandra Coelho. *Algumas notas sobre as novas tecnologias de informação e comunicação e o contrato de teletrabalho subordinado*. In Scientia Iuridica, n.º 335, 2014.

MOREIRA, Teresa Alexandra Coelho. *A privacidade dos trabalhadores e o controlo electrónico da utilização da Internet*. In Questões Laborais, n.ºs 35-36, 2011.

MOREIRA, Teresa Coelho. "*As Novas Tecnologias de Informação e Comunicação: um Adminirável Mundo Novo no Trabalho*". In: Revista de Direito e Garantias Fundamentais, Vitória, n° 11, 2012.

MOREIRA, Teresa Alexandra Coelho *L'impatto delle nuove tecnologie nella conciliazione tra vita e lavoro*. Revista Labour and Law Issues. 2017.

NOVAIS P., CARNEIRO D., *Interdisciplinary Perspectives on Contemporary Conflict Resolution*, IGI-Global, 363 pages, ISBN: 978-1-5225-0245-6, 2016. Disponível em: http://dx.doi.org/10.4018/978-1-5225-0245-6 .

PIMENTA A., CARNEIRO D., NOVAIS P., NEVES J., *Detection of Distraction and Fatigue in Groups through the Analysis of Interaction Patterns with Computers*, *Intelligent Distributed Computing VIII*, Springer-Verlag - Studies in Computational Intelligence, David Camacho, Lars Braubach,

Salvatore Venticinque and Costin Badica (Eds) Vol. 570, pp 29-39, ISBN: 978-3-319-10421-8, 2014. Disponível em: http://dx.doi.org/10.1007/978-3-319-10422-5_5.

PORTUGAL. *Tribunal de Contas de Portugal. Publicações*. Disponível em: <https://www.tcontas.pt/ptpt/TribunalContas/Publicacoes/ColetaneasLegislacao>.

RIVERO, Jean; WALINE, Jean. "*Os princípios fundamentais do serviço público*". Droit Administratif', Français. Précis Dalloz, 14 édition, p. 388-389, 1992.

ROUVROY, A. "*Privacy Data Protection and the Unprecedented Challenges of Ambient Intelligence*". In: "*Studies in Ethics, Law and Technology*". v. 2 (1), 2008.

SANTOS, Fabiola Meira de Almeida; TALIBA, Rita. *Lei Geral de Proteção de Dados no Brasil e os possíveis impactos*. Revista dos Tribunais On-line, São Paulo, v. 998, p. 4, 2018.

SETZER, Valdemar W.; SILVA, Flávio Soares Corrêa da. *Banco de dados: Aprenda o que são, melhore seu conhecimento, construa os seus*. São Paulo: Edgard Blücher. p. 48, 2005.

SHARDA, Ramesh; DURSUN, Delen e TURBAN, Efraim. *Business Intelligence and Analytics: Systems for Decision Suport*, 10th Edition, Hardcover, 2014;

SILVEIRA, Alessandra. Cidadania e direitos fundamentais. In: SILVEIRA, Alessandra; CANOTILHO, Mariana; FROUFE, Pedro (Coord.). *Direito da União Europeia. Elementos de direito e políticas da União*. Coimbra: Almedina, 2016.

SILVEIRA, Alessandra. *Princípios de direito da União Europeia*. Lisboa: Quid Juris, 2012.

SILVEIRA, Alessandra. *TRATADO DE LISBOA*. Versão Consolidada. Quid Juris. 4 ed. Fevereiro/2019.

SOMBRA, Thiago Luís Santos. *Fundamentos da regulação da privacidade e proteção de dados pessoais: pluralismo jurídico e transparência em perspectiva*. São Paulo: Thomson Reuters Brasil, p. 172, 2019.

TOFFOLI, José Antonio Dias - na abertura do *"Seminário sobre a Lei Geral de Proteção de Dados: a caminho da efetividade"*, realizado no Superior Tribunal de Justiça - STJ em parceria com outros órgãos e entidades - Julho, 2019. Disponível em: <https://stj.jusbrasil.com.br/noticias>. Acessado em: 10 de dez. de 2019.

UNIÃO EUROPEIA. *RGPD: Diretrizes, recomendações e melhores práticas*. Disponível em: <https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_pt > Acessado em: 21 de nov.de 2019.

VERONESE, Alexandre; MELO, Noemy. *O Projeto de Lei 5.276/2016 em contraste com o novo Regulamento europeu (2016/679 UE)*. Revista de Direito Civil Contemporâneo, v. 14, p. 71-99, 2018.

VERONESE, Alexandre. In: *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro* [livro eletrônico]. Org. Ana Frazão, Gustavo Tepedino, Milena Donato Oliva coordenação. São Paulo: Thomson Reuters Brasil, Parte I, Cap. 14, p. 1, 2019.

Legislação

BRASIL. *Constituição da República do Brasil*. Texto Oficial. Planalto. Brasília. 2018.

BRASIL. Lei n° 12.965, de 23 de abril de 2014. *Regula o uso da Internet no Brasil. Marco Civil da Internet*. Disponível em: <http://www.planalto.gov.br/> Acessado em: 18 de dez. de 2019.

BRASIL. Lei n° 13.709, de 14 de agosto de 2018. *Lei Geral de proteção de Dados Pessoais*. Disponível: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> Acessado em: 10 de dez. de 2019.

BRASIL. Senado Federal. Legislação. Norma. Disponível em: <www.senado.gov.br>

BRASIL. Projeto de Lei (PL) 4060, de 2012. *Dispõe sobre o tratamento de dados pessoais*. de 14 de agosto de 2018.*Lei Geral de proteção de Dados Pessoais.*Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=>. Acessado em: 17 de jan. de 2020.

BRASIL. STF – *Constituição da República Federativa do Brasil*. Disponível em: <www.stf.jus.br/constituição>

BRASIL. Tribunal de Contas do Estado da Paraíba. *Legislação do TCE/PB. Texto Oficial*. <www.tce.pb.gov.br>

BRASIL. *Lei no 12.527, de 18 de novembro de 2011*. Diário Oficial da República Federativa do Brasil Brasilia, DF, 18 nov. 2011. Disponível em: <http://www.planalto.gov.br/ccivil03/ato2011-2014/2011/lei/l12527.htm>.

BRASIL. *Tribunal de Contas do Estado do Rio Grande do Norte.* Legislação do TCE/RN. Texto oficial. <www.tce.rn.gov.br>
Legislação e Jurisprudência do Tribunal de Contas de Portugal. Disponível em: www.tcontas.pt/pt/publicacoes/manuais_publicacoes.shtm

PORTUGAL. ANACOM – Autoridade Nacional de Comunicações. Legislação. Disponível em: <https://www.anacom.pt/>. Acessado em: 21 de abr. de 2019.

PORTUGAL. CNPD – Comissão Nacional de Proteção de Dados. Decisões. Disponível em: < https://www.cnpd.pt/bin/decisoes/Delib/DEL_2019_495.pdf)->. Acessado em: 21 de abr. de 2019.

PORTUGAL. Lei n° 26, de 22 de agosto de 2016. Disponível em: <www.dre.pt/pesquisa>. Acessado em: 12 de dez. de 2019.

PORTUGAL. Lei n° 58/2019, de 8 de agosto de 2019, a qual assegura a execução do RGPD na ordem jurídica nacional, Disponível em: <https://dre.pt/web/guest/pesquisa/>. Acessado em: 20 de nov. de 2019.

UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:pt:HTML>. Acessado em: 15.jan. de 2020.

UNIÃO EUROPEIA. Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (privacidade e às comunicações eletrónicas"). Disponível em: <https://eur-lex.europa.eu/legalcontent/PT/TXT/?uri=CELEX%3A32002L0058> Acessado em: 14 de fev. de 2020.

UNIÃO EUROPEIA. Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.o 45/2001 e a Decisão n.o 1247/2002/CE (JO L 295 de 21.11.2018, p. 39-98). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1594414075505&uri=CELEX:32018R1725>.
Acessado em: 06 de fev. de 2020.

Trabalhos Acadêmicos

DOMINGOS, T. B. *Um Processo para Analise de Segurança em Software*. 2000. 156 f. Dissertação (Mestrado em Computação) - Departamento de Computação, Universidade Federal de Alagoas, Maceió, 2000.

MONTEIRO, Ana Carolina da Mota. *Videovigilância: Privacidade e Segurança – Análise Especial da Situação do Trabalhador.* Mestrado em Direitos Humanos. 2015. 192 f. Universidade do Minho, Braga, 2015.

PICKCIUS, Raul Denis. *As Novas Tecnologias como Instrumentos de Controle externo da Administração Pública pelas Cortes de Contas.* Mestrado em Ciência Jurídica. 2018. 142 f. Universidade do Vale do Itajaí – UNIVALI. Itajaí/SC, 2018.

SILVA, André Gustavo Almeida e. *A Relação entre Transparência Pública e Gestão Fiscal nos Municípios Brasileiros.* 75 f. Dissertação apresentada ao Programa de Pós-graduação em Administração (PPGA) – UFRN, Natal/RN, 2019.

Outros documentos - Links pesquisados

ATRICON – Associação dos Membros dos Tribunais de Contas do Brasil. Disponível em: <http://www.atricon.org.br/institucional/apresentacao/>.

Sociedade de Vigilância. BIG DATA. Disponível em: <https://www.academia.edu/40236159/Responsabilidade_civil_de_administradores_de_sociedades_empres%C3%A1rias_por_decis%C3%B5es_tomadas_com_base_em_sistemas_de_inteligi%C3%AAncia_artificial>.

Manual de Gestão de Riscos do TCU. Disponível em: <https://drive.google.com/file/d/1YEHkCaLgyfg3qxW6tJxOxER-Q1YTte8d/view>.

CNIL - Autoridade de Proteção de Dados da França. Disponível em: <www.cnil.fr/en/home>

Significados. Disponível em: < https://www.significados.com.br/url/> .

TRAMITA-SUPORTE – Tribunal de Contas da Paraíba. Disponível em: <www.tce.pb.gov/tramita>.

SAGRES-CAPTURA. Disponível em: <https://tce.pb.gov.br/servicos/sagres-captura>

SISPATRI-TCE/RN. Disponível em: http://www.tce.rn.gov.br/SisPatrimonio/Index>

ICP Brasil. ICP Brasil, ou Infraestrutura de Chaves Públicas Brasileira. Disponível em: <https://www.iti.gov.br/icp-brasil>.

Instituto Rui Barbosa – IRB. Disponível em: <www.irbcontas.org.br>

Consulta à Legislação da Europa. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32016R0679>

Princípios do RGPD - Disponível em: <https://blog.kwanko.com/pt-pt/dados-pessoais-rgpd-esta-pronto/>

BRASIL. Câmara dos Deputados. Projeto de Lei (PL) nº 4.060, de 2012. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=>. Acessado em: 17 de jan. de 2020.

Parlamento-Portugal. Disponível em: <www.parlamento.pt/actividadeparlamentar>

Plano Estratégico TC. de Portugal. Disponível em: <https://www.tcontas.pt/pt-pt/Transparencia/PlaneamentoGestao/PlanosTrienais/Documents/plano_estrategico_vf_internet_hp_20191106.pdf>.

Flávia Lefèvre Guimarães. Advogada especializada em direito do consumidor, telecomunicações e direitos digitais Disponível em: <https://flavialefevre.com.br/pt/about>.

Rafael Pellon de Lima Sampaio. Advogado especialista em Internet, Mídia e Entetenimento – Disponível em: <https://www.jusbrasil.com.br/topicos/29291674/rafael-pellon-de-lima-sampaio>.

BRASIL. Guia de Transparência Ativa para Órgãos e Entidades do Poder Executivo Federal - 6ª Versão – 2019. Disponível em: <www.acessoainformacao.gov.br/lai-para-sic/guias-e-orientacoes/gta-6a-versao-2019.pdf>.

BRASIL. Informações sobre o Governo eletrônico – *egov.* Disponível em: <https://www.infoescola.com/informatica/governo-eletronico/>

Cidade Inteligente ou Smart Cities. Disponível em: <https://fgvprojetos.fgv.br/noticias/o-que-e-uma-cidade-inteligente>

UNIÃO EUROPEIA. Consulta à legislação da União Europeia. Disponível em: <https://eur-lex.europa.eu/legal>

Núcleo de Informação e Coordenação do Ponto BR - Comitê Gestor da Internet no Brasil – CGI-br. Disponível em: <https://www.nic.br/>

Direitos na Rede. Disponível em: <www.direitosnarede.org.br>

Sobre a Cambridge Analytica Ltda. Consulta à página do Sítio Jus Brasil. Disponível em: <https://www.jusbrasil.com.br/topicos/187366730/cambridge-analytica>.

Conceitos e definições. Disponível em: <https://pt.wikipedia.org/wiki/>

Sobre "bolhas ideológicas". Disponível em: <https://jornalggn.com.br/eleicoes/bolhas-ideologicas-ou-camaras-de-eco-por-fernando-nogueira-da-costa>

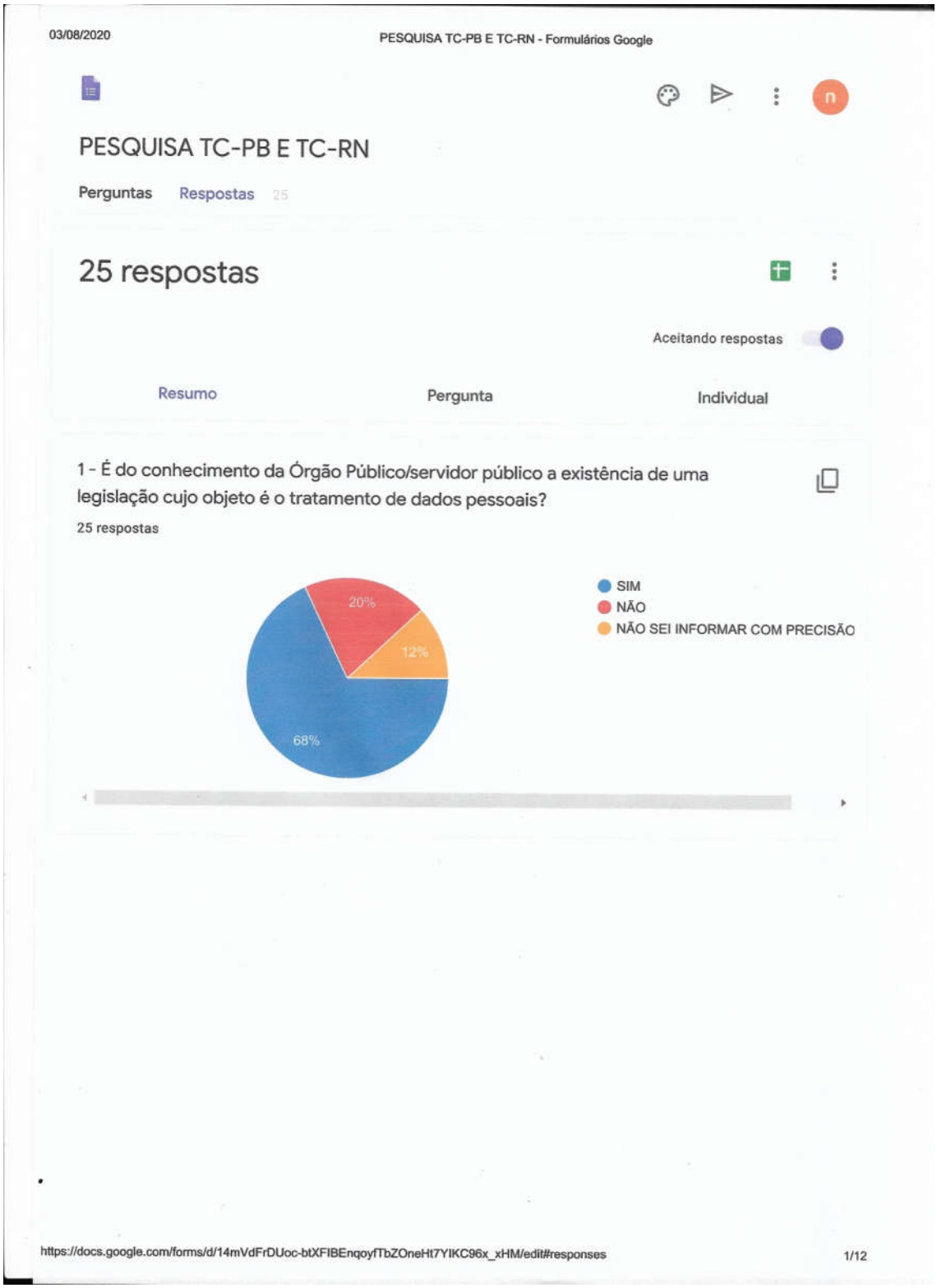
Colégio Notarial do Brasil - Seção Paraná. Sobre a Autoridade Nacional de Proteção de Dados. Disponível em: <https://cnbpr.org.br/2019/07/11/artigo-as-mudancas-finais-da-lei-geral-de-protecao-de-dados-pessoais/>
Ferramenta RevelaGov. São Paulo.Brasil. Disponível em: <https://www.revelagov.com/>.

Qual é o SGBD que se adapta melhor ao seu projeto? Disponível em: <https://meunegocio.uol.com.br/academia/tecnologia/mysql-x-sql-server-x-mongodb-x-postgres--qual-banco-de-dados-escolher.html#rmcl>.

Portal brasileiro de dados abertos. "O que são dados abertos?". Disponível em: <http://www.dados.gov.br/pagina/dados-abertos>. Acessado em: 20 de jan. de 2020.

Ferramenta RevelaGov. São Paulo. Brasil. Disponível em: <https://www.diariofm.com.br/noticia/projeto-de-ribeirao-anticorrupcao-e-selecionado-em-desafio-na-onu>

ANEXOS


03/08/2020
PESQUISA TC-PB E TC-RN - Formulários Google
PESQUISA TC-PB E TC-RN
Perguntas
Respostas 25
25 respostas
Aceitando respostas
Resumo
Pergunta
Individual
1 - É do conhecimento da Órgão Público/servidor público a existência de uma legislação cujo objeto é o tratamento de dados pessoais?
25 respostas
20%
12%
68%
SIM
NÃO
NÃO SEI INFORMAR COM PRECISÃO
https://docs.google.com/forms/d/14mVdFrDUoc-btXFIBEnqoyfTbZOneHt7YIKC96x_xHM/edit#responses
1/12

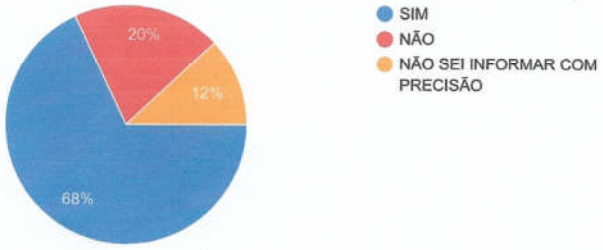
PESQUISA SOBRE LGPD

25 respostas

Publicar análise

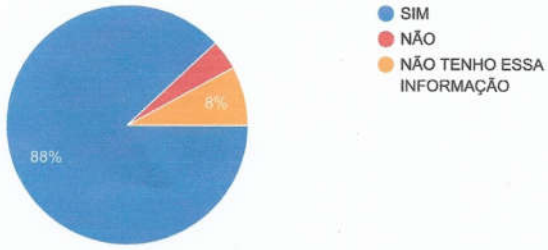
GERAL

25 respostas



2 - O Órgão Público possui ferramenta de pesquisa de conteúdo que permita o acesso à informação?

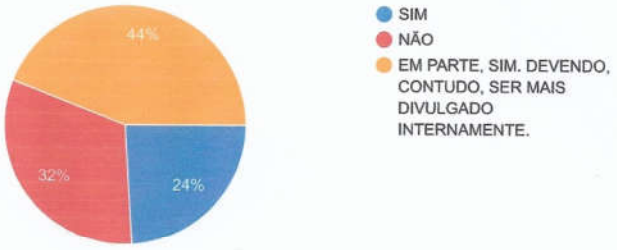
25 respostas



INFORMAÇÃO

3 - Para os efeitos de tratamento legal, é claro para o servidor público o conceito e os tipos de informação manuseadas pela área de Tecnologia da Informação?

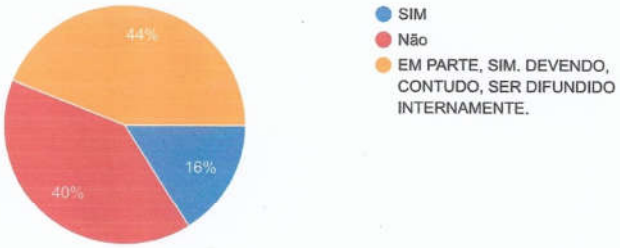
25 respostas



DADOS

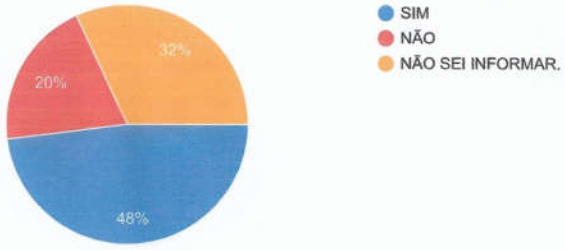
4 - Para os efeitos de tratamento legal, é claro para o servidor público o conceito e os tipos de dados manuseados pela área de Tecnologia da Informação?

25 respostas



5 – O banco de dados está concentrado na área de Tecnologia da Informação ou está distribuído em vários locais do Órgão Público?

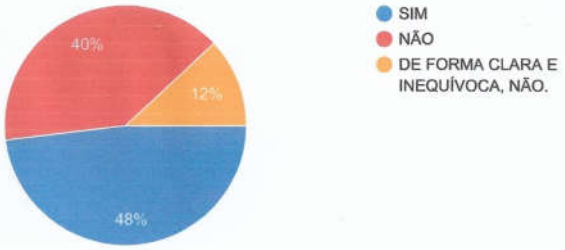
25 respostas



TRATAMENTO DE DADOS

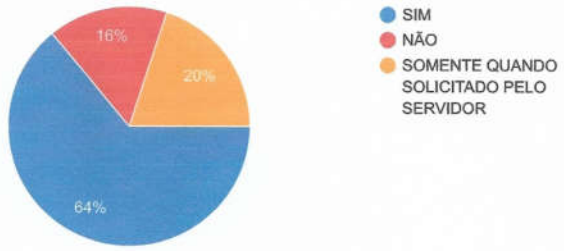
6 – Os servidores titulares de dados são previamente informados acerca da finalidade para a qual seus dados são tratados?

25 respostas



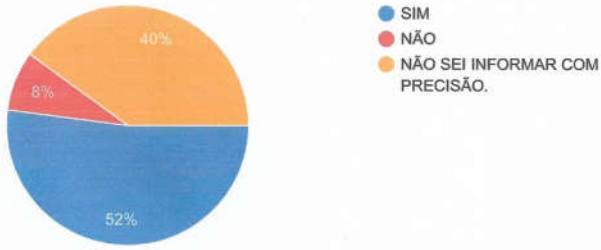
7 – É garantido o livre acesso bem como a integralidade dos dados pessoais aos seus titulares?

25 respostas



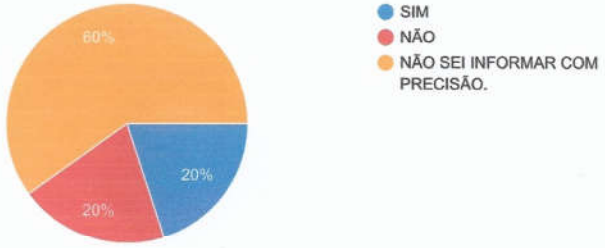
8 – Há utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais autorizados e não autorizados e de situações acidentais ou ilícitas de destruição, perda etc?

25 respostas



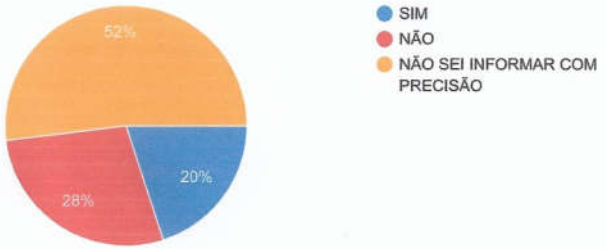
9 - Existe algum estudo ou mesmo ferramenta no sentido de garantir o prévio consentimento do titular para que os seus dados sejam tratados, inclusive quanto aos dados pessoais sensíveis?

25 respostas



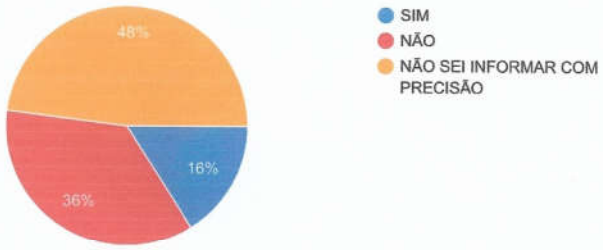
10 – Existe um encarregado pelas operações de tratamento de dados pessoais?

25 respostas



11 – Em seu sítio eletrônico (do Tribunal), há alguma informação clara e atualizada acerca da previsão legal, da finalidade e dos procedimentos e práticas utilizadas no tratamento de dados pessoais?

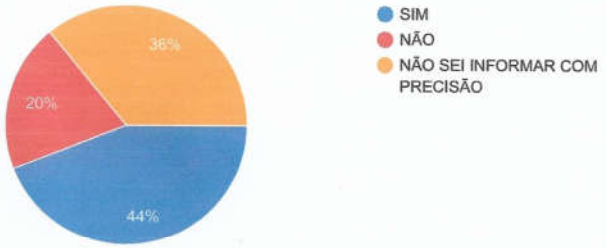
25 respostas



COMPARTILHAMENTO DE DADOS

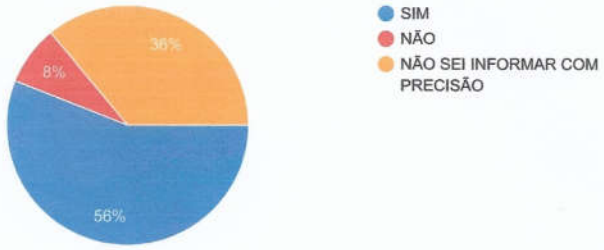
12 - O Órgão compartilha dados pessoais com terceiros? Observadas as hipóteses: 12.1 - Para execução descentralizada de atividade pública

25 respostas



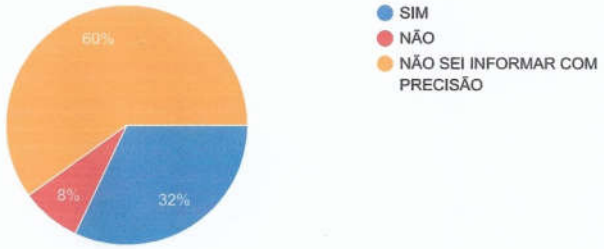
12 - O Órgão compartilha dados pessoais com terceiros? Observadas as hipóteses: 12.2 - Em virtude de contratos, convênios ou de previsão legal

25 respostas



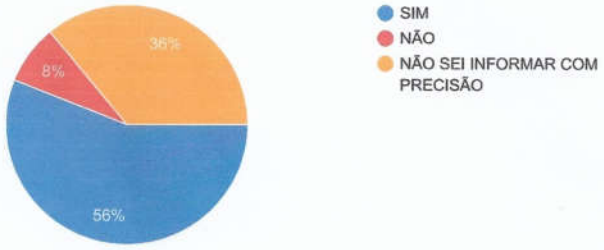
12 - O Órgão compartilha dados pessoais com terceiros? Observadas as hipóteses: 12.3 - Para prevenção de fraudes e irregularidades ou para proteger e resguardar a segurança e integridade do titular dos dados

25 respostas



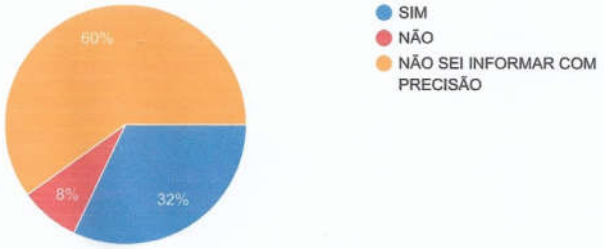
12 - O Órgão compartilha dados pessoais com terceiros? Observadas as hipóteses: 12.2 - Em virtude de contratos, convênios ou de previsão legal

25 respostas



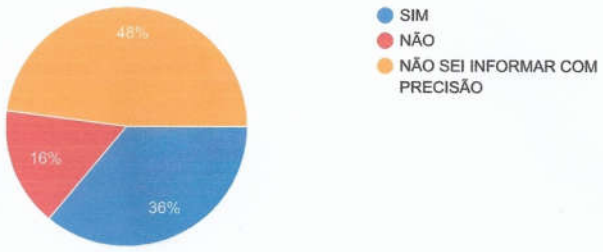
12 - O Órgão compartilha dados pessoais com terceiros? Observadas as hipóteses: 12.3 - Para prevenção de fraudes e irregularidades ou para proteger e resguardar a segurança e integridade do titular dos dados

25 respostas



12 - O Órgão compartilha dados pessoais com terceiros? Observadas as hipóteses: 12.4 - No caso dos dados serem acessíveis publicamente

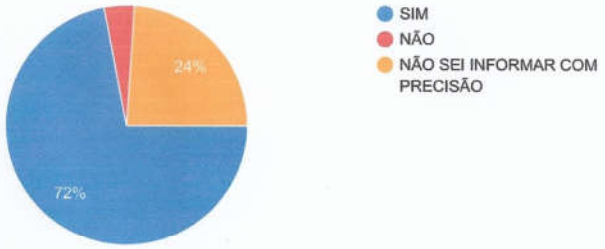
25 respostas



PUBLICAÇÃO DE RELATÓRIO/ACESSO À INFORMAÇÃO

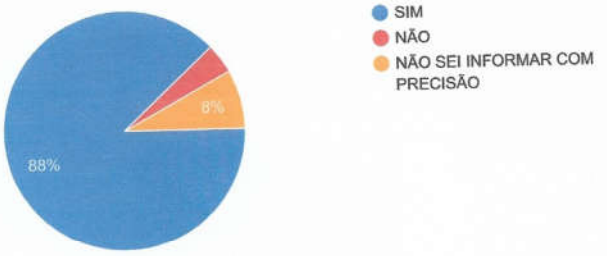
13 - O Site do Órgão possibilita a gravação de relatórios em diversos formatos eletrônicos, abertos e não proprietários, tais como planilhas e texto (CSV), de modo a facilitar a análise das informações?

25 respostas



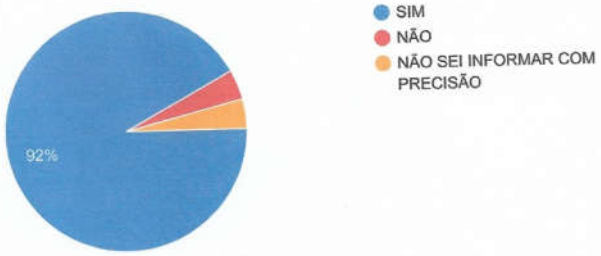
14 – O site possibilita a obtenção de informações relativas à: 14.1 - Administração do patrimônio público, utilização de recursos públicos, licitação, contratos administrativos?

25 respostas



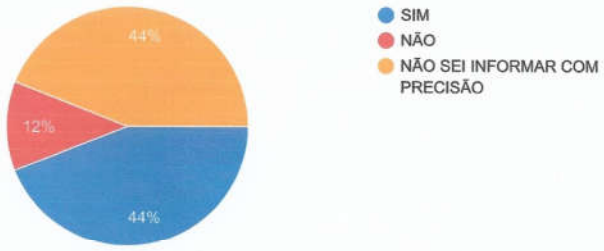
14 – O site possibilita a obtenção de informações relativas à: 14.1 -Ao resultado de inspeções, auditorias, prestação e tomadas de contas realizadas em seus jurisdicionados?

25 respostas



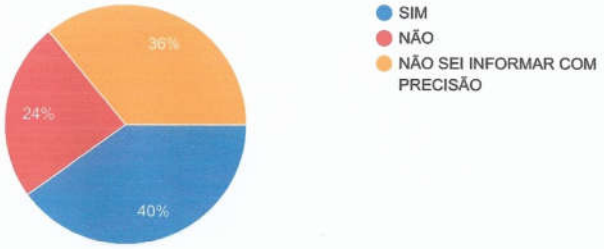
15 – Nos processos de Auditoria, constam apenas as informações relevantes diretamente relacionadas com o objeto e âmbito da auditoria, preservando-se os dados pessoais?

25 respostas



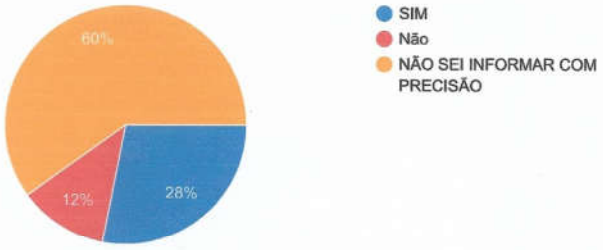
16 – Nos processos de denúncia, há a proteção dos dados pessoais do denunciante e denunciado até a decisão definitiva de mérito?

25 respostas



17 – Nos processos de Consulta dos Relatórios dos órgãos de controlo interno que contenham dados pessoais, são assegurados procedimentos de segurança ou até mesmo restrição do acesso à informação?

25 respostas



18 – Ao publicar as suas decisões, o Tribunal de Contas tem observado as regras de limitação e conservação dos dados pessoais, que permitem a identificação de seus titulares, atendendo apenas ao período necessário as finalidades para as quais são tratados?

25 respostas