UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
UNIDADE ACADÊMICA DE GRADUAÇÃO
CURSO DE DIREITO

JOÃO CAETANO DE FREITAS D`AVILA

COREIA DO SUL E JAPÃO: DIFERENÇAS NORMATIVAS NA PROTEÇÃO DE DADOS E SEUS REFLEXOS NA DECISÃO DE ADEQUAÇÃO DA UNIÃO EUROPEIA

Porto Alegre/RS
2021

João Caetano de Freitas D`Avila

COREIA DO SUL E JAPÃO: DIFERENÇAS NORMATIVAS NA PROTEÇÃO DE DADOS E SEUS REFLEXOS NA DECISÃO DE ADEQUAÇÃO DA UNIÃO EUROPEIA

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do título de Bacharel em Ciências Jurídicas e Sociais, pelo Curso de Direito da Universidade do Vale do Rio dos Sinos (UNISINOS).

Orientador: Prof. Dr. Gabriel Pessin Adam

Porto Alegre/RS

2021

Dedico este trabalho a todos que fazem e já fizeram parte de minha família, pois sou quem eu sou especialmente por conta de vocês.

AGRADECIMENTOS

Escrever uma monografia, tal qual qualquer trabalho de caráter acadêmico, é um processo essencialmente dialógico. Portanto, os agradecimentos aqui tecidos conferem a importância para efetivação deste processo tão relevante.

Agradeço imensamente ao professor Gabriel Pessin Adam, meu orientador, por ter aceito me acompanhar na jornada de produção desta monografia. O empenho e dedicação a mim dispensados foram essenciais para o desenvolvimento deste trabalho, através da constante disponibilidade e valiosas lições.

Expresso minha gratidão a todos os professores do curso de Direito da UNISINOS Porto Alegre (LES) por me fornecerem as bases necessárias a minha formação profissional e à realização deste trabalho, aos quais agradeço com profunda admiração. Em especial, agradeço ao professor Marcos Catalan por colaborar com o meu processo de amadurecimento intelectual, e ao professor Wilson Engelmann pelos seus aconselhamentos acadêmicos, e por ter contribuído na construção do conhecimento que tenho hoje quanto às tecnologias.

Também agradeço aos meus colegas do curso de Direito, pelo companheirismo e ajuda na construção do aprendizado que tenho hoje. Tenho muita gratidão pelas amizades construídas ao longo dos 5 anos de curso de graduação.

Por fim, a minhas avós, Luiza por todo o carinho que me dá e Vani por todo o carinho que me deu. E especialmente a minha eterna gratidão a meus amados país, Ana Luiza e Bláir, pelo amor incondicional e por sempre me ajudarem diante dos obstáculos que a vida me apresenta.

A todos vocês, deixo registrado meu mais profundo sentimento de gratidão, pois sei que sem a ajuda de vocês não seria capaz de redigir esta monografia.

"Direito é sistema de regras, sistema lógico, que satisfaz as exigências metalógicas de coerência, ou lógicas de consistência. As regras jurídicas hão de construir sistema. Nenhuma regra jurídica é sòzinha, é gôta, ainda quando tenha sido o artigo ou parágrafo único de uma lei. Caïria, como gôta, no copo cheio de líquido colorido, e a sua côr juntar-se-ia às das outras gotas que lá se pingaram noutros momentos."[1]

[1] MIRANDA, Pontes de. **Comentários à Constituição de 1946.** Rio de Janeiro: Editor Borsoi, 3.ª Edição, Tomo I (Arts 1.º - 5º), 1960. p. 33.

RESUMO

Esta investigação coteja os sistemas de proteção de dados japonês e sul-coreano, partindo da hipótese de que o impacto desempenhado pelo instituto de proteção de dados detém diferenças quanto à implementação e aplicação nos dois ordenamentos em questão. Para averiguar tal pressuposto, estabelece-se como problema de pesquisa demarcar as principais diferenças entre as legislações de proteção de dados do Japão e da Coreia do Sul e o modo como as possíveis divergências entre os dois ordenamentos influenciariam na decisão de adequação da Comissão Europeia. Para tanto, o estudo adotou metodologia comparativa qualitativa, a partir de uma análise de configurações de condições, investigando os fenômenos como processos de condições relacionais, configuradas a partir da inserção no contexto sob estudo. Tecida a inspeção entre os ordenamentos, constataram-se divergências estruturais consideráveis entre os sistemas de proteção de dados japonês e sul-coreano e seus impactos na decisão de adequação da União Europeia. Quanto às distinções entre os ordenamentos, o japonês é mais brando quanto às responsabilidades de quem controla os dados e quanto aos direitos dos titulares; identidade que guarda consonância com a bagagem cultural e os costumes morais nipônicos. Por outro lado, e também por elemento cultural, o instituto de proteção de dados sul-coreano detém vieses rígidos quanto à proteção de dados. Tal característica é originária dos períodos de domínio militar, em que foram mantidos aparelhos de vigilância estatal muito forte sobre a população, resultando em uma estrutura de normas de proteção de dados completa e rigorosa, para a defesa dos titulares. Acerca dos impactos dessas características na decisão de adequação, no caso do Japão, os modelos adotados, não obstante baseados em conceitos ocidentais, estão igualmente calcados em princípios culturais locais; o que pode gerar complexidades quanto à proteção de dados entre União Europeia e esse país. Em contrapartida, no caso da Coreia do Sul, há clara convergência da cultura local às normas originadas na UE; o que garante uma maior segurança diante da proteção de dados entre o bloco e essa última nação. Por fim, destaque-se que a proteção e a regulação do instituto de proteção de dados constituem fator indispensável para o equilíbrio entre o interesse econômico e a proteção da privacidade do indivíduo.

Palavras-chave: Proteção de Dados; Japão; Coreia do Sul; Decisão de Adequação da Comissão Europeia; Trânsito de Dados entre Países.

ABSTRACT

This investigation compares the Japanese and South Korean data protection systems, starting from the hypothesis that the impact performed by the data protection institute holds differences in terms of implementation and application in the two systems in question. The research problem devised to verify the hypothesis stems from marking out the main differences between Japan and South Korea's data protection legislation and understanding how possible divergences between the two legal systems would influence the European Commission's adequacy decision. The study adopted a qualitative comparative methodology, based on an analysis of configurations of conditions, investigating the phenomena as processes of relational needs configured from their insertion in the context under study. After the inspection of the two legal orders, considerable structural divergences were found between the Japanese and South Korean data protection systems and their impacts on the European Union's adequacy decision. As for the distinctions between the regulations, the Japanese one is more lenient regarding the responsibilities of those who control the data and the holders' rights, an identity in line with the Japanese cultural baggage and moral customs. On the other hand, and also for cultural reasons, the South Korean data protection institute has strict biases regarding data protection. This characteristic originates from a period of military domination in which intense state surveillance devices were maintained on the population, resulting in a structure of complete and rigorous data protection norms for the defense of the holders. Regarding the impacts of these characteristics on the adequacy decision, in the case of Japan, the adopted models, despite being based on Western concepts, are equally based on local cultural principles, which can generate complexities in terms of data protection between the European Union and the latter country. On the other hand, in the case of South Korea, there is apparent convergence of local culture to norms originating in the EU, which guarantees greater security regarding data protection between the block and the latter nation. Finally, it should be noted that the safety and regulation of the data protection institute is an indispensable factor for the balance between the economic interest and the protection of an individual's privacy.

Keywords: Data Protection; Japan; South Korea; European Commission Adequacy Decision; Transit of Data between Countries.

LISTA DE SIGLAS

CCC	Comissão de Comunicações da Coreia
CDP	Controladores de Dados Pessoais
CEDH	Convenção Europeia de Direitos Humanos
CPIP-CS	Comissão de Proteção de Informações Pessoais da Coreia do Sul
CPIP-JP	Comissão de Proteção de Informações Pessoais do Japão
CSF	Comissão de Serviços Financeiros
EUA	Estados Unidos da América
ICO	Information Commissioner's Office
LPIP-CS	Lei de Proteção de Informações Pessoais da Coreia do Sul
LPIP-JP	Lei de Proteção de Informações Pessoais do Japão
LUPIC	Lei de Uso e Proteção de Informações de Crédito
NRR	Número de Registro de Residente
OCDE	Organização para Cooperação e Desenvolvimento Econômico
PSIC	Provedores de Serviços de Informação e Comunicação
RCPI	Rede de Comunicação e Proteção da Informação
RGPD	Regulamento Geral de Proteção de Dados
UE	União Europeia

SUMÁRIO

1 INTRODUÇÃO

A circulação de dados caracteriza a época em que vivemos e se expande cada mais rapidamente nos contextos de transmissão de informação. A quarta revolução industrial remete a um mundo no qual os dados se tornam cada vez mais sensíveis, evidenciando a necessidade de agir dos ordenamentos jurídicos;[2] especialmente após um momento de grandes migrações digitais, devido à pandemia do COVID-19, período em que o processo de migração de dados vem sendo acelerado.[3] É nessa condição que o presente trabalho se propõe a analisar o instituto da proteção de dados nos ordenamentos jurídicos japonês e sul-coreano. Seguindo as peculiaridades individuais históricas, geográficas e sociais de cada país, o instituto da proteção de dados é elemento acolhido pelas legislações de ambas as nações eleitas para este estudo. Com o expoente crescimento das economias de plataforma por todo o mundo, o trânsito de dados, tanto no âmbito internacional quanto no nacional, nunca foi tão intenso, o que, por consequência, salienta a necessidade da proteção de uso.[4]

A União Europeia (UE) se destaca como expoente no campo da proteção de dados, tendo originado a base legal adotada em praticamente todo o mundo por deter um dos ordenamentos legais mais completos sobre o tema.[5] O Japão foi considerado pela UE zona em *compliance* no tratamento de dados, e a Coreia do Sul está em processo para o mesmo efeito.[6] Esses elementos surgem mesmo inexistindo uma organização intergovernamental regional que cubra a região do Nordeste da Ásia, onde se localizam. Ambos os países, contudo, apresentam importantes características culturais partilhadas, como influências confucionistas e budistas e estão próximos no âmbito político, tendo histórias jurídicas comuns, nas quais o direito civil desempenha um papel preponderante. [7]

---

[2] SCHWAB, Klaus. **A Quarta Revolução Industrial.** Tradução de Daniel Moreira Miranda. São Paulo: Edipro, 2016. p. 105.

[3] INFORMATION COMMISSIONER'S OFFICE (ICO). **The Information Commissioner's response to the International Trade Committee Inquiry into Digital Trade and Data**. 2021. p.1. Disponível em: https://ico.org.uk/media/about-the-ico/consultation-responses/2619342/itc-digital-trade-data-response-202002.pdf. Acesso em: 26 de set. de 2021.

[4] TRINDADE, Manoel Gustavo Neubarth. **Economia de Plataforma (Ou Tendência à Bursatilização dos Mercados): Ponderações Conceituais Distintivas em Relação à Economia Compartilhada e à Economia Colaborativa e uma Abordagem de Análise Econômica do Direito dos Ganhos de Eficiência Econômica por Meio da Redução Severa dos Custos de Transação.** Lisboa: Revista Jurídica Luso-Brasileira (RJLB), Ano 6, N.º 4, 2020. p. 1986 e 1987.

[5] LYNSKEY, Orla. **The Foundations of EU Data Protection Law.** Oxford: Oxford University Press, 2015. passim.

[6] EUROPEAN COMMISSION. **Adequacy decisions How the EU determines if a non-EU country has an adequate level of data protection.** 2021. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Acesso em: 27 de set. de 2021.

[7] GREENLEAF, Graham. **Asian Data Privacy Laws: Trade & Human Rights Perspectives.** Oxford: Oxford University Press, 2014. E-book/Kindle Edition. p. 28 e 29.

Tanto o Japão quanto a Coreia do Sul são reconhecidos pela UE em relação à confiança de procedimentos em tratamentos de dados. Já sendo o Japão considerado como zona de tratamento de alto nível no que se refere a dados, em 16 de junho de 2021, a Comissão Europeia deu inicio ao procedimento para a adoção de uma "decisão de adequação" das transferências de dados pessoais para a Coreia do Sul, ao abrigo do Regulamento Geral de Proteção de Dados (RGPD).[8] Tal garantia cria um sistema de livre trânsito de dados, em que as barreiras burocráticas não são necessárias. O Japão; portanto, representa o único país asiático a ser considerado zona de trânsito seguro de dados até agora; contudo, não o único reconhecido, segundo manifestação da Comissão Europeia.[9]

Frente a tal realidade, o problema de pesquisa que guiará a presente monografia é assim estabelecido: Quais são as principais diferenças entre as legislações de proteção de dados do Japão e da Coreia do Sul e como tais divergências influenciam na decisão de adequação da Comissão Europeia?

Tendo em vista o problema de pesquisa exposto, o objetivo geral da monografia é investigar quais são as principais diferenças entre as legislações de proteção de dados do Japão e da Coreia do Sul e se elas impactam na decisão de adequação declarada pela Comissão Europeia.

Como objetivos específicos, são selecionados os seguintes aspectos:

(a) apresentar o conceito de proteção de dados;

(b) descrever a evolução da proteção de dados na União Europeia; e

(c) contextualizar histórica e socialmente a adoção das legislações de proteção de dados no Japão e na Coreia do Sul.

A hipótese a partir da qual se constrói esta investigação é a de que o impacto desempenhado pela proteção de dados detém diferenças quanto à implementação e aplicação em ambas as nações analisadas. Tal pressuposição se estabelece principalmente a partir da noção desses países compartilharem uma variedade de características, a exemplo de questões culturais, históricas, religiosas e jurídicas, bem como por se tratarem de atuais expoentes mundiais no campo dos avanços tecnológicos em geral.[10] Portanto, é relevante aprofundar o

---

[8] EUROPEAN COMMISSION. **Data protection: European Commission launches the process towards adoption of the adequacy decision for the Republic of Korea.** 2021. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964. Acesso em: 27 de set. 2021

[9] Id. **Adequacy decisions How the EU determines if a non-EU country has an adequate level of data protection.** 2021. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Acesso em: 27 de set. de 2021.

[10] WIPO. **Global Innovation Index 2021: Tracking Innovation throught the COVID-19 Crisis.** Geneva: World Intellectual Property Organization, 2021. p. 4. Acesso em: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2021.pdf. Disponível em: 10 de nov. de 2021.

entendimento sobre o estudo do tema da proteção de dados, para que se possa compreender as características e as diferenças que o instituto possui no Japão e Coreia do Sul, bem como para melhor reconhecer a inserção do mesmo aos princípios emanados pela Comunidade Europeia, expoente absoluto no tema.

Assim, o estudo tratará da análise dos dois ordenamentos jurídicos (Japão e Coreia do Sul) sob a luz do instituto da proteção de dados, tecendo uma comparação, a fim de identificar possíveis pontos divergentes, bem como observando impactos no que tange às relações nacionais e internacionais, públicas e privadas. Dito de outro modo, a meta desta investigação é de compreender o papel desempenhado pelo instituto, sob a ótica dos ordenamentos jurídicos em questão, buscando constatar se as características desses levam a decisões de adequação diversas emitidas pela Comissão Europeia.

A escolha do tema se fundamenta nos elementos de identidade histórica, cultural e jurídica semelhantes entre Japão e Coreia do Sul, tendo em vista o reconhecimento que estas nações recebem pela UE no que se refere à transmissão e tratamento de dados. Este fato decorre clara e especialmente por serem os dois países expoentes nos avanços tecnológicos mundiais.

Para realizar a investigação do instituto entre tais ordenamentos, adota-se a metodologia comparativa qualitativa, para tecer comparação de casos, a partir de uma análise de configurações de condições, pensando os fenômenos não como resultantes de um conglomerado de variáveis independentes, mas como processo de condições relacionais que são configuradas a partir da inserção no contexto sob estudo. Assim, o trabalho está divido em 6 capítulos: (i) Introdução, (ii) Proteção de Dados, (iii) Japão, (iv) Coreia do Sul, (v) Análise Comparativa Entre o Sistema de Proteção de Dados do Japão e da Coreia do Sul, e (vi) Considerações Finais.

Na sequência dessa introdução, o 2º capítulo detalhará a temática de proteção de dados, apresentando a relevância do instituto, o histórico e a decisão de adequação emitida pela Comissão Europeia. O 3º capítulo abordará especificamente o contexto do Japão, enquanto o 4º capítulo tratará da Coreia do Sul. A análise das leis nacionais de privacidade de dados, por sua vez, será desenvolvida tanto no capítulo 3 quanto no 4, baseada na seguinte organização: (i) contexto histórico e político de privacidade de dados; (ii) contexto de vigilância; (iii) sistema legal; (iv) normas de privacidade de dados; e (v) caso concreto. No 5º capítulo, será estabelecido um comparativo acerca das normas de privacidade de dados entre a Coreia do Sul e o Japão, observando os possíveis impactos diante da decisão de adequação da União Europeia. Tal análise será guiada pelos mesmos tópicos citados acima para os capítulos

3 e 4. Por fim, as considerações finais tecerão reflexões sobre a trajetória geral das normas de privacidade em ambos os ordenamentos e as possíveis influências na decisão de adequação, por parte da Comissão Europeia, assim com discutirão o modo como o desenvolvimento dessas normas esclarece as questões levantadas neste estudo.

Em síntese, o presente trabalho busca evidenciar, considerando valores e interesses atinentes à proteção da privacidade de dados, aspectos relevantes do ordenamento jurídico e às práticas do Japão e da Coreia do Sul neste cenário. Além disto, analisaremos as diferenças em relação ao tratamento do tema e as influências no processo de decisão de adequação emitido pela Comissão Europeia.

2 A PROTEÇÃO DE DADOS

A instituição da proteção jurídica de dados que se pretende explorar no presente capítulo, a relevância da mesma, o conceito de privacidade presente em tal instituto e o desenvolvimento até o momento atual, é elemento de primeira ordem na conjuntura social contemporânea, no mundo todo. Com o advento da WEB (Internet), que integrou intensamente a maioria dos países do mundo – se não todos -, acarretando aos cidadãos a sujeição - e estes passaram a ser, também, sujeitos desta relação - às atividades de monitoramento de empresas predominantemente sediadas em outros países, em particular, mas não exclusivamente, nos EUA. Neste cenário, as legislações então existentes para a privacidade de dados se tornam ineficientes para lidar com isso. O mesmo se aplica à operação internacional de agências de segurança de alguns países, mais uma vez, em particular, mas não exclusivamente, os EUA. Os temores do setor privado e da vigilância estatal aumentam, o "fluxo livre de dados" internacional tem crescimento intenso e, ao mesmo tempo, isto se torna muito mais difundido e com grande valoração.

2.1 Relevância da proteção de dados na contemporaneidade

Em meio à Quarta Revolução Industrial, é nítida a migração de prioridades entre as infraestruturas físicas e digitais, além das relações da diferença de utilização de elementos já existentes em um outro ambiente, mais especificamente para os fins desse trabalho, de dados.[11] Nesse sentido, de acordo com Vanessa Jiménez Serranía[12]:

> No século 20, o valor mudou de infraestruturas físicas, como terrenos e fábricas, para intangíveis, como marcas e propriedade intelectual. Estes agora se expandem para dados, o que está se tornando um importante ativo corporativo, um fator econômico vital e a base de novos modelos econômicos.

Tal questão é igualmente evidenciada pela matéria da "*The Economist*" com o titulo sugestivo: O recurso mais valioso do mundo não é mais o óleo, mas os dados (tradução

[11] SCHWAB, Klaus. **A Quarta Revolução Industrial.** Tradução de Daniel Moreira Miranda. São Paulo: Edipro, 2016. passim.

[12] SERRANÍA, Vanessa Jiméz; ABRUSIO, Juliana. **Big Data: Uma Análise Sob A Óptica Das Práticas Abusivas No Acesso E Uso De Dados Massificados Na Economia De Plataforma.** Florianópolis: Revista de Direito Brasileira, v. 28, Nº. 11, 2021. p. 390.

nossa). Conforme evidenciado pelo artigo, dados nunca tiveram tanto valor quanto têm agora, dada a abrangência da aplicabilidade desses.[13]

Assim, o desenvolvimento acelerado da tecnologia traz novos desafios para a proteção de dados no mundo, uma vez que houve uma intensificação das fontes captadoras e geradoras de dados. Os avanços tecnológicos em banco de dados, estatísticas, mecanismos de buscas, em "*machine learning"* (aprendizado de máquina) e em "*data mining"* (mineração de dados), são alguns dos elementos que viabilizam as ferramentas como o "Big Data"[14], utilizada mundialmente tanto pelo setor público quanto pelo privado, além do crescente mercado de tecnologias *"smart"*. Por meio de tais ferramentas, os dados são adquiridos, transmitidos, armazenados e analisados das mais diversas formas, sendo usados para diversos fins, especialmente econômicos.[15] A tecnologia nunca demandou por tantos dados dos usuários. Este fenômeno, que apenas aumenta com o passar dos anos, pode ser denominado como "comoditização dos dados". [16]

Exemplo de tais impactos são encontrados nas mais diversas áreas, tais quais: campanhas de varejo, publicidade, seguros, estratégia de investimento, entretenimento e política. Através de publicações em redes sociais, questionários e compras de produtos, por exemplo, tais dados são captados. O que permite, por meio dessas tecnologias citadas acima, que os dados sejam coletados nas mais diversas circunstâncias e situações, visando um aumento do desempenho a partir da análise de tais dados.[17]

Grandes corporações "de dados", como o Facebook – uma das companhias com maior avaliação na história dos EUA –, basicamente obtêm lucro captando e processando dados de usuários, sem cobrar destes pelo uso dos sistemas, pois justamente comercializam os dados

---

[13] "The world's most valuable resource is no longer oil, but data". THE ECONOMIST. **The world´s most valuable resource is no longer oil, but data.** 2017. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 1 de nov. 2021.

[14] *"O termo big data foi cunhado pela área de marketing para descrever grandes e diversos conjuntos de informações que estão crescendo a uma taxa cada vez maior devido ao próprio desenvolvimento da sociedade da informação e das interações empresariais e pessoais. O termo descreve o grande volume de dados – estruturados e não estruturados – e está relacionado tanto aos avanços na mineração de dados (data mining), quanto ao surpreendente aumento do poder computacional e à capacidade de armazenamento de dados, que possibilitam análises e correlações mais sofisticadas. O termo big data começou a ser utilizado, timidamente, no início dos anos 90, e seu emprego aumentou exponencialmente com o passar dos últimos anos sendo que passou a ser considerado como estratégico para o desenvolvimento de um negócio nos dias atuais."* SERRANÍA, Vanessa Jiméz; ABRUSIO, Juliana. **Big Data: Uma Análise Sob A Óptica Das Práticas Abusivas No Acesso E Uso De Dados Massificados Na Economia De Plataforma.** Florianópolis: Revista de Direito Brasileira, Florianópolis (RDBF), v. 28, Nº. 11, 2021. p. 390.

[15] Ibid., p. 390 e 391.

[16] LYNSKEY, Orla. **The Foundations of EU Data Protection Law.** Oxford: Oxford University Press, 2015. p. 1, 2 e 3.

[17] SERRANÍA, op cit., p. 390.

das pessoas que fazem uso das plataformas aos verdadeiros “clientes”; ou seja, às demais empresas que possuam interesse de marketing e/ou comercialização de produtos aos usuários. Como é dito hoje em dia: “se o produto é de graça, você é o produto”.[18]

Neste ambiente de intensa digitalização das relações entre as pessoas, e destas com os mercados, a padronização dos contratos conjugado com a listagem de ofertas, forjam a Economia de Plataforma. Em outras palavras, a centralização das ofertas dos agentes econômicos participantes dentro de uma determinada plataforma, que consubstanciam mercados virtuais, padronizados e ordenados, com funcionamento ininterrupto, permitindo comparações e escolhas imediatas e automatizadas. O elemento indispensável deste universo, e sua razão de ser, são os dados.[19]

Diante do atual cenário, a legislação para proteger a privacidade em relação às informações pessoais evoluiu de forma bastante consistente em todo o mundo. A proteção de dados é consequência natural como forma de garantia da cidadania. Uma vez percebidos os impactos do uso de dados no nosso relacionamento com os negócios, mercados e até mesmo com a sociedade. As legislações relativas à privacidade de dados têm contribuído muito para o desenvolvimento da consciência coletiva para a relevância e o respeito à privacidade das informações pessoais dos cidadãos.[20]

2.2 História da regulação da proteção de dados

A Lei de Dados da Suécia de 1973 se tornou a primeira legislação nacional a contemplar a proteção de dados sob norma positiva, tendo incluído a maioria dos elementos do que atualmente consideramos ser uma lei de proteção de dados.[21] Naquela época, o Parlamento Europeu evidenciou a grande necessidade do desenvolvimento da legislação nesse tema, devido ao aumento crescente do processamento de dados nas indústrias europeias.[22]

---

[18] LYNSKEY, Orla. **The Foundations of EU Data Protection Law.** Oxford: Oxford University Press, 2015. p. 2 e 3.

[19] TRINDADE, Manoel Gustavo Neubarth. **Economia de Plataforma (Ou Tendência à Bursatilização dos Mercados): Ponderações Conceituais Distintivas em Relação à Economia Compartilhada e à Economia Colaborativa e uma Abordagem de Análise Econômica do Direito dos Ganhos de Eficiência Econômica por Meio da Redução Severa dos Custos de Transação.** Lisboa: Revista Jurídica Luso-Brasileira (RJLB), Ano 6, N.º 4, 2020. passim.

[20] EUROPEAN COMMISSION. **Adequacy decisions How the EU determines if a non-EU country has an adequate level of data protection.** 2021. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Acesso em: 27 de set. de 2021.

[21] GREENLEAF, Graham. **Asian Data Privacy Laws: Trade & Human Rights Perspectives.** Oxford: Oxford University Press, 2014. E-book/Kindle Edition. p. 6.

[22] EUROPEAN PARLIAMENT. **Resolution on the Protection of the Rights of the Individual in the Face of Developing Technical Profess in the Field of Automatic Data Processing**. 1982. Disponível em:

Em sequência, a partir da década de 1980, são editadas as Diretrizes de Privacidade da Organização para Cooperação e Desenvolvimento Econômico (OCDE)[23] não vinculantes e o primeiro acordo internacional vinculativo, a Convenção de Proteção de Dados do Conselho da Europa,[24] ambos incorporaram princípios de privacidade substancialmente semelhantes. Estas diretrizes estabeleceram que uma nação seria considerada como possuidora de legislação de Proteção de Dados apenas na hipótese desta normatização ser editada pelos mecanismos legislativos deste mesmo país, e desde que previssem, em relação às atividades do setor privado, ou do próprio setor público - ou ambos – um conjunto básico de regulamentação de privacidade de dados, seus princípios e padrões, incluindo, no mínimo, a maior parte das Diretrizes da OCDE ou da Convenção do Conselho da Europa, além de alguns métodos de aplicação obrigatória por lei; ou seja, não apenas autorregularão, mas legislação cogente.[25]

A proteção de dados também recebe guarida legislativa de outras normas que acessoriamente são agregadas às leis específicas do tema. Mesmo com variações particulares aos países de origem, estas leis podem e são aplicadas de forma conexa às de privacidade de dados. Como exemplo, estão incluídas as previsões legais para delitos de privacidade, quebra de confiança, assim como direitos constitucionais, leis de limitação de vigilância e, especialmente, leis de proteção ao consumidor. Da mesma forma, muitos acordos internacionais de direitos humanos estabelecem direitos ou determinam a criação de direitos nas nações aderentes a eles, estabelecendo, assim, fatores de proteção à privacidade.[26] Exemplo disto, é o Artigo 17 do Pacto Internacional sobre Direitos Civis e Políticos[27], diretamente relevante para ambos os ordenamentos a serem abordados nesse estudo, que o Brasil é signatário através do Decreto nº 592, de 6 de julho de 1992, *in verbis:*

---

https://op.europa.eu/en/publication-detail/-/publication/37a4ff25-4e1a-494f-bf8d-db860627910a/language-en. Acesso em: 1 de out. de 2021.

[23] ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD). **Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.** 1980. Disponível em: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Acesso em: 2 de out. de 2021.

[24] COUNCIL OF EUROPE. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (European Treaty Series No. 108.)** 1981. Disponível em: https://rm.coe.int/1680078b37. Aceso em: 4 de set. de 2021.

[25] GREENLEAF, Graham. **Asian Data Privacy Laws: Trade & Human Rights Perspectives.** Oxford: Oxford University Press, 2014. E-book/Kindle Edition. p. 6.

[26] Ibid., p. 7.

[27] NAÇÕES UNIDAS. **Pacto Internacional de Direitos Civis e Políticos**. (Decreto nº 592) Brasília, DF: Presidência da República, 1992. Disponível em: http://legislacao.planalto.gov.br/legisla/legislacao.nsf/Viw_Identificacao/DEC%20592-1992?OpenDocument. Acesso em: 4 de out. de 2021.

> ARTIGO 17
> 1. Ninguém poderá ser objetivo de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honra e reputação.
> 2. Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas.

A atual circunstância social de integração tecnológica entre as nações, nem de perto imaginada em 1966, quando da edição do acordo internacional de proteção aos direitos civis e políticos, direcionou paulatinamente as políticas legislativas das nações, na medida de sua evolução, para os patamares hoje encontrados. De qualquer forma, a complementariedade entre as normas de direitos humanos e civis, é elemento indissociável da moderna proteção de dados implementada na maioria dos países democráticos.[28] Aqui, é interessante frisar, a posição dos EUA que, apesar da supremacia econômica, da relevância das empresas do país e das políticas internacionais manterem forte peso no mundo, essa nação, por não deter uma lei nacional de privacidade de dados cobrindo o setor privado, cada vez mais fica isolada, e isso a coloca em uma posição não privilegiada na tentativa de influenciar padrões globais de privacidade de dados.[29] Tal aspecto, conforme destacado anteriormente, dá ainda mais poder à EU, quanto ao pioneirismo e experiência em relação ao manejo e proteção de dados.

A integração dos países asiáticos com a proteção de dados se dá através da própria integração com o ocidente no pós-guerra, onde os vínculos comerciais e de sinergia entre os atores econômicos cada vez mais necessitaram de acolhimento nas regras tanto nacionais quanto nas internacionais. A partir de então, as leis de proteção de dados foram se tornando onipresentes em diversos países pelo mundo. Isto ocorreu, inclusive e especialmente, nos países asiáticos, democráticos, com atuação de ponta no segmento tecnológico, visto a intersecção relevante desses nos meios de tratamento de dados operados mundialmente.[30]

Neste cenário, as Diretrizes de Privacidade da OCDE (1980) foram uma das primeiras influências no desenvolvimento de leis de privacidade de dados na Ásia.[31] Desde de 1988, o Japão passou a ter Lei sobre a Proteção de Informações Pessoais Detidas por Órgãos Administrativos. Já na Coreia do Sul, a proteção de dados cobrindo o setor público ocorreu 1995, através da Lei de Proteção de Dados de Agências Públicas. Ambos os países, como

---

[28] GREENLEAF, Graham. **Asian Data Privacy Laws: Trade & Human Rights Perspectives.** Oxford: Oxford University Press, 2014. E-book/Kindle Edition. passim.
[29] Ibid. p. 7 e 8.
[30] Ibid. passim.
[31] ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD). **Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.** 1980. Disponível em: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Acesso em: 02 de out. de 2021.

membros da OCDE, ao cobrir apenas os setores públicos, implementaram abordagem semelhante a alguns outros membros da OCDE de fora da Europa, tais quais, Austrália (1988) e Canadá (1982).[32]

Entre 2012 e 2013 houve um grande processo de desenvolvimento de leis de privacidade de dados na Ásia. Leis de privacidade de dados já existentes passaram por revisões, as quais promoveram avanços para o instituto. Desta forma, foi dado início a uma "segunda geração" de leis de privacidade de dados mais rígidas.[33] Conforme será abordado em maior profundidade nos capítulos 3 e 4, novas normativas foram desenvolvidas na Coreia do Sul e no Japão. Nesse último, inclusive, foi criado um núcleo como autoridade de proteção de dados que propôs as primeiras revisões importantes da lei geral, tendo realizado atualizações constantes até a data do presente estudo.

É importante observar que, conforme tais legislações bebem da fonte Europeia, existe um complicador da importação de regras legais de um país para outro, o que já ocorreu algumas vezes na realidade desses dois ordenamentos. Por exemplo, grande parte do sistema jurídico japonês vem de legislações estrangeiras: (a) a adoção da lei comercial Alemã no final do século XIX; e (b) a adoção da lei corporativa dos Estados Unidos em 1950.[34] Tal influência ocidental, por sua vez, teve como efeito o aceite de modo indireto dessa tradição jurídica pela Coreia.[35]

Considerando que as leis de privacidade de dados se originaram a partir de bases ocidentais, tanto a Coreia do Sul quanto o Japão foram países com profundos e históricos contatos com o ocidente. Esse fator, torna ambos os países como os mais próximos das questões ocidentais na Ásia.[36] Além disso, é importante frisar que a conjunto de regras legais que caracterizam uma lei de privacidade de dados não foi encontrado em nenhuma outra nação na Ásia antes de 1988, nessa sentido Greenleaf[37] constata que:

---

[32] GREENLEAF, Graham. **Asian Data Privacy Laws: Trade & Human Rights Perspectives.** Oxford: Oxford University Press, 2014. E-book/Kindle Edition. p. 9 e 10.

[33] Ibid., p. 11.

[34] NISHITANI, Yuko. **Introdução à História do Direito Japonês.** Tradução do alemão, de Maitê Schmidtz, Luciana Quinto e revisão da Profa. Dra. Cláudia Lima Marques. Porto Alegre: Revista da Faculdade de Direito da Universidade Federal do Rio Grande do Sul, 2002. p. 84, 85, 86, 87 e 88.

[35] KWON, Youngjoon. **Korea: Bridging the Gap between Korean Substance and Western Form.** Cambridge: Cambridge University Press, Law and Legal Institutions in Asia, E. Ann Black E Gary F. Bell, Eds., 2011, p. 151.

[36] GREENLEAF, Graham. **Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories.** Sydney: 23(1) Journal of Law, Information & Science, University of New South Wales (UNSW Sydney), 2013. p. 11.

[37] "The collection of legal rules that characterize a data privacy law was not to be found anywhere in characterize a data privacy law was not to be found anywhere in Asia prior to 1988, and any of the laws enacted up to the early 1990s would be unlikely to have been enacted if it were not for the existence of the OECD Privacy Guidelines. Since the mid-1990s, the EU Data Protection Directive 26 (the 'EU Directive') has been at least as

> A coleção de regras legais que caracterizam uma lei de privacidade de dados não foi encontrada em nenhum lugar na Ásia antes de 1988, e qualquer uma das leis promulgadas até o início dos anos 1990 dificilmente teria sido promulgada se não fosse pela existência das diretrizes de privacidade da OCDE. Desde meados da década de 1990, a Diretiva de Proteção de Dados da UE teve uma influência pelo menos tão forte quanto as Diretrizes da OCDE na região (tradução nossa).

Na Europa, a União Europeia tem papel fundamental para a unificação e desenvolvimento da proteção de dados.[38] A Ásia, por sua vez, não possui nenhuma união semelhante ao da UE, o que fez com que os movimentos legislativos se dessem de forma diferente. Como salienta Greenleaf[39]:

> De qualquer modo, na Ásia não existem tratados vinculativos equivalentes à Convenção 108 do Conselho da Europa sobre Proteção de Dados, ou ao Artigo 8 da Convenção Europeia de Direitos Humanos (CEDH) ou outros instrumentos obrigatórios, como a proteção de dados "constitucional" da UE ou a Diretiva da UE. Não existem tribunais internacionais que possam tomar decisões vinculativas em questões relacionadas com a proteção de dados, ao contrário do Tribunal de Justiça Europeu (TJCE ou TJUE) em questões como se os Estados-Membros da UE implementaram adequadamente a Diretiva (por exemplo, os casos sobre a independência autoridades de proteção de dados), ou o Tribunal Europeu dos Direitos do Homem (TEDH) sobre a interpretação do artigo 8.º da CEDH (tradução nossa).

Assim, na Ásia, não há acordos internacionais vinculativos sobre privacidade de dados, com exceção do Artigo 17 do Pacto Internacional sobre Direitos Civis e Políticos de 1966, equivalente ao Artigo 8 da CEDH. O que mais se aproxima disso em ambos os países, é a tentativa do "fluxo livre" de dados pessoais no interesse de facilitar o comércio e o desejo dos Estados e dos cidadãos de ter as informações pessoais protegidas por pelo menos um

---

strong an influence as the OECD Guidelines." GREENLEAF, Graham. **Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories.** Sydney: 23(1) Journal of Law, Information & Science, University of New South Wales (UNSW Sydney), 2013. p. 12.

[38] KUNER, Christopher. **European Data Protection Law: Corporate Compliance and Regulation.** Oxford: Oxford University Press, 2nd Edition, 2007. passim.

[39] "However, in Asia there are no binding treaties equivalent to Council of Europe Data Protection Data Protection Convention 108, or Article 8 of the ECHR or other mandatory instruments like the EU's 'constitutional' data protection, 28 or the EU Directive. There are no international courts which can make binding decisions on issues relating to data protection, unlike the European Court of Justice (ECJ or CJEU) on questions such as whether EU member states have properly implemented the Directive (for example, the cases on independence of data protection authorities), or the European Court of Human Rights (ECtHR) on the interpretation of Article 8 of the ECHR". GREENLEAF, Graham. **Asian Data Privacy Laws: Trade & Human Rights Perspectives.** Oxford: Oxford University Press, 2014. E-book/Kindle Edition. p. 13.

padrão mínimo acordado, independentemente de para onde esses dados foram transferidos. Modelo o qual a União Europeia tenta adotar hoje no mundo.[40]

2.3 Decisão de adequação pela Comissão Europeia

De modo a contextualizar um dos pressupostos estruturantes desse estudo, é importante compreender o papel desempenhado pela União Europeia para o instituto da proteção de dados e da capacidade da UE em determinar decisões de adequação. Conforme evidenciado previamente, a UE é expoente quanto a proteção de dados no mundo contemporâneo. Além disso, é o maior bloco econômico do mundo que, pela atual valoração de dados, possui significativa vantagem quanto ao manejo e tratamento dos mesmos.

Podemos definir adequação, segundo o ICO (Information Commisionar's Office)[41], autoridade independente de proteção de dados do Reino Unido, como:

> Adequação é um termo utilizado pela UE para descrever outros países, territórios, setores ou organizações internacionais que considera fornecer um nível de proteção de dados "essencialmente equivalente" ao que existe na UE. Uma decisão de adequação é uma decisão formal tomada pela UE que reconhece que outro país, território, setor ou organização internacional oferece um nível de proteção de dados pessoais equivalente ao da UE (tradução nossa).

Após a caracterização do que é uma adequação, a ICO[42] caracteriza propriamente o que é uma decisão de adequação, como: "Uma decisão de adequação é uma decisão formal tomada pela UE que reconhece que outro país, território, setor ou organização internacional oferece um nível de proteção de dados pessoais equivalente ao da UE" (tradução nossa).

Portanto, o efeito da decisão de adequação é que os dados pessoais podem fluir livremente entre um país terceiro para a União Europeia sem que seja necessária qualquer

---

[40] EUROPEAN COMMISSION. **Adequacy decisions How the EU determines if a non-EU country has an adequate level of data protection.** 2021. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Acesso em: 27 de set. de 2021.

[41] "'Adequacy' is a term that the EU uses to describe other countries, territories, sectors or international organisations that it deems to provide an 'essentially equivalent' level of data protection to that which exists within the EU." INFORMATION COMMISSIONER'S OFFICE (ICO). **Adequacy.** 2021. Disponível em: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/adequacy/. Acesso em: 1 de nov. de 2021.

[42] "An adequacy decision is a formal decision made by the EU which recognises that another country, territory, sector or international organisation provides an equivalent level of protection for personal data as the EU does." INFORMATION COMMISSIONER'S OFFICE (ICO). **Adequacy.** 2021. Disponível em: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/adequacy/. Acesso em: 1 de nov. de 2021.

salvaguarda adicional. Em outras palavras, as transferências serão equiparadas a transmissões de dados intra-UE.[43]

De modo a determinar se um país fora da UE oferece um nível adequado de proteção de dados, a Comissão Europeia faz uso do teor do Artigo 45.º do RGPD para estabelecer os critérios de adequação para o tratamento de dados pessoais e à livre circulação desses. Os dois primeiros itens (números) do Artigo 45[44] estabelecem os parâmetros para a avaliação da decisão de adequação pela Comissão Europeia; *in verbis*:

> Art. 45. Transferências com base numa decisão de adequação
> 1. Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica.
> 2. Ao avaliar a adequação do nível de proteção, a Comissão tem nomeadamente em conta os seguintes elementos:
> a) O primado do Estado de direito, o respeito pelos direitos humanos e liberdades fundamentais, a legislação pertinente em vigor, tanto a geral como a setorial, nomeadamente em matéria de segurança pública, defesa, segurança nacional e direito penal, e respeitante ao acesso das autoridades públicas a dados pessoais, bem como a aplicação dessa legislação e das regras de proteção de dados, das regras profissionais e das medidas de segurança, incluindo as regras para a transferência ulterior de dados pessoais para outro país terceiro ou organização internacional, que são cumpridas nesse país ou por essa organização internacional, e a jurisprudência, bem como os direitos dos titulares dos dados efetivos e oponíveis, e vias de recurso administrativo e judicial para os titulares de dados cujos dados pessoais sejam objeto de transferência;
> b) A existência e o efetivo funcionamento de uma ou mais autoridades de controlo independentes no país terceiro ou às quais esteja sujeita uma organização internacional, responsáveis por assegurar e impor o cumprimento das regras de proteção de dados, e dotadas de poderes coercitivos adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e cooperar com as autoridades de controlo dos Estados-Membros; e
> c) Os compromissos internacionais assumidos pelo país terceiro ou pela organização internacional em causa, ou outras obrigações decorrentes de convenções ou instrumentos juridicamente vinculativos, bem como da sua participação em sistemas multilaterais ou regionais, em especial em relação à proteção de dados pessoais.

---

[43] EUROPEAN COMMISSION. **Adequacy decisions How the EU determines if a non-EU country has an adequate level of data protection.** 2021. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Acesso em: 27 de set. de 2021.

[44] UNIÃO EUROPEIA. **Regulamento (UE) 2016/679, de 27 de abril de 2016.** Institui na União Europeia o Regulamento Geral sobre a Proteção de Dados**.** UE: Parlamento Europeu e o Conselho da União Europeia, Art. 45, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Acesso em: 10 de out. de 2021.

Como pode ser visto acima, os primeiros dois itens do transcrito Artigo, estabelecem as condições para a decisão de adequação. Em sequência, o Artigo 45[45], nos itens seguintes, determina quais as medidas de controle a serem adotadas pela Comissão Europeia após a avaliação da decisão de adequação para continuar a garantir o nível de segurança quanto ao fluxo de dados:

> 3. Após avaliar a adequação do nível de proteção, a Comissão pode decidir, através de um ato de execução, que país terceiro, um território ou um ou mais setores específicos de um país terceiro, ou uma organização internacional, garante um nível de proteção adequado na aceção do n.º 2 do presente artigo. O ato de execução prevê um procedimento de avaliação periódica, no mínimo de quatro em quatro anos, que deverá ter em conta todos os desenvolvimentos pertinentes no país terceiro ou na organização internacional. O ato de execução especifica o âmbito de aplicação territorial e setorial e, se for caso disso, identifica a autoridade ou autoridades de controlo a que se refere o n.º 2, alínea b), do presente artigo. O referido ato de execução é adotado pelo procedimento de exame a que se refere o artigo 93.º, n.º 2.
> 4. A Comissão controla, de forma continuada, os desenvolvimentos nos países terceiros e nas organizações internacionais que possam afetar o funcionamento das decisões adotadas nos termos do n.º 3 do presente artigo e das decisões adotadas com base no artigo 25.º, n.º 6, da Diretiva 95/46/CE.
> 5. A Comissão, sempre que a informação disponível revelar, nomeadamente na sequência da revisão a que se refere o n.º 3 do presente artigo, que um país terceiro, um território ou um ou mais setores específicos de um país terceiro, ou uma organização internacional, deixou de assegurar um nível de proteção adequado na aceção do n.º 2 do presente artigo, na medida do necessário, revoga, altera ou suspende a decisão referida no n.º 3 do presente artigo, através de atos de execução, sem efeitos retroativos. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 93.º, n.º 2.
> Por imperativos de urgência devidamente justificados, a Comissão adota atos de execução imediatamente aplicáveis pelo procedimento a que se refere o artigo 93.º, n.º 3.
> 6. A Comissão inicia consultas com o país terceiro ou a organização internacional com vista a corrigir a situação que tiver dado origem à decisão tomada nos termos do n.º 5.
> 7. As decisões tomadas ao abrigo do n.º 5 do presente artigo não prejudicam as transferências de dados pessoais para o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou para a organização internacional em causa, nos termos dos artigos 46.º a 49.º.
> 8. A Comissão publica no Jornal Oficial da União Europeia e no seu sítio web uma lista dos países terceiros, territórios e setores específicos de um país terceiro e de organizações internacionais relativamente aos quais tenha declarado, mediante decisão, se asseguram ou não um nível de proteção adequado.

[45] UNIÃO EUROPEIA. **Regulamento (UE) 2016/679, de 27 de abril de 2016.** Institui na União Europeia o Regulamento Geral sobre a Proteção de Dados, UE: Parlamento Europeu e o Conselho da União Europeia, Art. 45, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Acesso em: 10 de out. de 2021.

> 9. As decisões adotadas pela Comissão com base no artigo 25.º, n.º 6, da Diretiva 95/46/CE permanecem em vigor até que sejam alteradas, substituídas ou revogadas por uma decisão da Comissão adotada em conformidade com o n.º 3 ou o n.º 5 do presente artigo.

Pelo que se depreende da leitura da norma acima, o objetivo central do normativo europeu sempre será evidenciar a aderência da norma do país de fora da Europa aos parâmetros legais de proteção de dados adotados pela UE. A norma estabelece as fronteiras necessárias para a fundamentação da decisão de adequação, inclusive podendo indicar alterações na lei do país em análise, buscando a aderência à lógica de defesa da UE de adoção global de elevados padrões de proteção de dados.[46]

Diante de tais parâmetros, a União Europeia já estabeleceu as duas primeiras avaliações de adequação de países ao abrigo do artigo 45.º do RGPD.[47] A primeira decisão em 2019 relativa ao Japão. Segundo a Comissária de Justiça, Consumidores e Igualdade de Gênero, Věra Jourová[48]:

> Esta decisão de adequação cria a maior área de fluxos de dados seguros do mundo. Os dados dos europeus se beneficiarão de altos padrões de privacidade quando seus dados forem transferidos para o Japão. Nossas empresas também se beneficiarão de um acesso privilegiado a um mercado de 127 milhões de consumidores. Investir em privacidade compensa; este acordo servirá como um exemplo para futuras parcerias nesta área-chave e ajudará a definir padrões globais (tradução nossa).

Assim, é importante salientar que esta decisão de adequação também complementa o Acordo de Parceria Econômica UE-Japão - que entrou em vigor em fevereiro de 2019. O que gera um grande beneficio entre as empresas de ambos os países quanto ao fluxo livre de dados. Assim, tirando proveito da era digital, facilitando o comércio internacional e a proteção dos dados entre ambos.[49]

---

[46] GREENLEAF, Graham. **The Draft Korea Adequacy Decision: Submission to European Union Authorities.** Sydney: University of New South Wales Law Research Series, 2021. p. 4.

[47] EUROPEAN COMMISSION. **Adequacy decisions How the EU determines if a non-EU country has an adequate level of data protection.** 2021. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Acesso em: 27 de set. de 2021.

[48] "This adequacy decision creates the world's largest area of safe data flows. Europeans' data will benefit from high privacy standards when their data is transferred to Japan. Our companies will also benefit from a privileged access to a 127 million consumers' market. Investing in privacy pays off; this arrangement will serve as an example for future partnerships in this key area and help setting global standards." EUROPEAN COMMISSION. **European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows.** 2019. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421. Acesso em: 10 de nov. de 2021.

[49] Ibid.

A segunda decisão de adequação, que não está no escopo proposto por esta monografia, ocorreu em 2021 e foi relativa ao Reino Unido. Contudo, este já estava em conformidade com os padrões de proteção de dados, e obteve a decisão de adequação devido à retirada da União Europeia.[50]

Por fim, a Coreia do Sul passa pelo processo de adequação, contudo a Comissão Europeia já concluiu que esse país garante um nível de proteção essencialmente equivalente ao garantido pelo RGPD. Assim, segundo relato mais recente da Comissão Europeia, o procedimento de efetivação da decisão de adequação com a Coreia do Sul será adotado o mais rapidamente possível nos próximos meses. [51]

Além disso, a decisão de adequação complementaria o Acordo de Livre Comércio UE-República da Coreia, o que tem o potencial de aumentar a cooperação entre a União Europeia e a Coreia do Sul, enquanto potências digitais. Este acordo comercial já levou a um aumento considerável no comércio bilateral de bens e serviços entre o bloco e a Coreia do Sul. Garantir o fluxo livre de dados pessoais para a República da Coreia por meio de uma decisão de adequação apoiará essa relação comercial estimada em quase € 90 bilhões.[52]

Assim, passamos à analise dos ordenamentos de proteção de dados no Japão e na Coreia do Sul, como únicos países fora da Europa reconhecidos pelos parâmetros do Art. 45 do RGPD. Destacaremos, também, como as diferenças presentes nos respectivos ordenamentos influenciaram e influenciam as respectivas decisões de adequação.

---

[50] EUROPEAN COMMISSION. **Data protection: Commission adopts adequacy decisions for the UK.** 2021. Disponível em: https://ec.europa.eu/commission/presscorner/detail/ro/ip_21_3183. Acesso em: 27 de set. de 2021.

[51] GREENLEAF, Graham. **The Draft Korea Adequacy Decision: Submission to European Union Authorities.** Sydney: University of New South Wales Law Research Series, 2021. p. 14.

[52] Ibid. p. 14.

3 JAPÃO

O Japão, como terceira maior economia em PIB nominal, décima primeira maior população do mundo, uma das democracias mais antigas da Ásia e, talvez, como elemento mais importante para esta análise, país líder nos avanços tecnológicos (Society 5.0), é um Estado de grande importância quanto à abordagem e futuro do Instituto da Proteção de Dados na Ásia e no mundo como um todo.[53] Conforme veremos a seguir, devido à natureza do ordenamento jurídico, além da legislação especifica, a proteção de dados deriva principalmente do suporte da matéria jurisprudencial e dos métodos alternativos de resolução de conflitos (Mediação, Arbitragem e Conciliação). Estes, por sua vez, moldam, paradigmaticamente, a orientação dos ministérios sobre como a legislação deve ser interpretada e aplicada;[54] fator incomum para uma nação cujas interações sociais tendiam, até recentemente, a encarar a intervenção do direito como "inútil e mesmo odiosa". Para a população média japonesa os costumes morais prescindem do direito.[55]

3.1 Sistema legal

O Direito Japonês sofreu uma grande influência do ocidente no sistema jurídico e cultural a partir de 1858.[56] Contudo, conservou uma marca de originalidade, devido ao caráter próprio dos japoneses e ao isolamento de 1641 até 1858 do período *Edo*.

A ideia de direito era ausente na sociedade primitiva nipônica. Em uma sociedade caracterizada pela clara divisão em classes, há repúdio à ideia de regulação da sociedade mediante regras jurídicas, o que era percebido como pouco flexível. Nesse cenário, desenvolveu-se um conjunto de regras que tomaram como base a moral da época e que regulavam, em todas as circunstâncias da vida, a conduta a ser seguida pelos indivíduos nas relações com os demais; tal conceito sendo fundamental para compreender até hoje as

---

[53] HIROSHI, Kajiyama. **Digital technology can help the world prosper. Here's how.** World Economic Forum**,** 2021. Disponível em: https://www.weforum.org/agenda/2021/04/digital-technology-can-help-the-world-prosper-gtgs/. Acesso em: 1 de set. de 2021.

[54] GREENLEAF, Graham. **Asian Data Privacy Laws: Trade & Human Rights Perspectives.** Oxford: University Press, 2014. E-book/Kindle Edition. p. 228

[55] DAVID, Renê. **Os Grandes Sistemas do Direito Contemporâneo**. Tradução por Hermínio A. Carvalho. São Paulo: Martins Fontes – selo Martins, 5ª. Ed, 2014. p. 607 e 608.

[56] NISHITANI, Yuko. **Introdução à História do Direito Japonês.** Tradução do alemão, de Maitê Schmidtz, Luciana Quinto e revisão da Profa. Dra. Cláudia Lima Marques. Porto Alegre: Revista da Faculdade de Direito da Universidade Federal do Rio Grande do Sul, 2002. p. 84.

relações jurídicas no país. Estas regras são denominadas *giri*.[57] O *giri*; por sua vez, funciona como um código de honra que molda a moral da população através de uma base ética para a cultura nipônica.[58] Tais regras foram fatores fundamentais observados na implementação de um novo sistema jurídico no país; reforma que adveio diante da necessidade de ocidentalização da nação, que, por razões de incremento comercial, optou, como referido acima, por inspirar-se no Direito Alemão. A inspiração se pautou nas grandes afinidades com a nação germânica, por exemplo, nas relações comerciais, através da noção de boa-fé. Além disso, a figura do *kaiser*, para fins jurídicos da época, guardava similaridades com a figura do Imperador.[59] E assim o ordenamento se manteve até a derrota japonesa na Segunda Guerra Mundial.

Após a derrota para os Aliados, o Japão adotou uma nova constituição em 1947, em grande medida imposta aos moldes dos Estados Unidos. As reformas mais substanciais foram, particularmente, no Direito Constitucional e no Processo Penal. Portanto, o sistema jurídico e os tribunais foram substancialmente influenciados pelos modelos tanto de Direito Civil Alemão, quanto pela *Commom Law* Americana. Assim, o sistema jurídico japonês apresenta quase um híbrido entre os dois sistemas, por mais que mantenha um ordenamento calcado na *Civil Law*.[60]

Além dessa fusão jurídica, como anteriormente referido, o sistema de leis japonês também é caracterizado por uma preferência pela arbitragem, mediação e conciliação de conflitos, como alternativa à solução judicial de disputas,[61] bem como por várias práticas administrativas que fornecem orientação aquém da lei formal.[62] Esse modelo organizacional entra em total consonância com o principio do *giri* e com a resistência quanto aplicação direta das normas jurídicas no país.

Ainda hoje, o Japão é uma democracia com um parlamento bicameral e uma monarquia constitucional com um imperador. Sendo um Estado unitário, não uma federação de estados, o país é legislado de forma centralizada; entretanto, o fato de os decretos

---

[57] FRADERA, Véra Maria Jacob de. **A Boa Fé Objetiva, uma noção presente no conceito alemão, brasileiro e japonês de contrato.** Porto Alegre: Revista Cadernos do Programa de Pós-Graduação em Direito PPGDir./UFRGS**,** 2003. p. 126.

[58] DAVID, Renê. **Os Grandes Sistemas do Direito Contemporâneo**. Tradução por Hermínio A. Carvalho. São Paulo: Martins Fontes – selo Martins, 5ª. Ed, 2014. p. 603.

[59] FRADERA, op cit., p 130.

[60] NISHITANI, Yuko. **Introdução à História do Direito Japonês.** Tradução do alemão, de Maitê Schmidtz, Luciana Quinto e revisão da Profa. Dra. Cláudia Lima Marques. Porto Alegre: Revista da Faculdade de Direito da Universidade Federal do Rio Grande do Sul, 2002. passim.

[61] JAPAN. **Act. No. 151 of 1 December 2004**. Act on Promotion of Use of Alternative Dispute Resolution. 2004. Disponível em: https://www.cas.go.jp/jp/seisaku/hourei/data/AOP.pdf. Acesso em: 15 de set. de 2021.

[62] CHIBA, Masaji. **Asian legal systems: law, society and pluralism in East Asia.** Ch. 3 in Tan (Ed.), 1997. passim.

necessitarem ser aprovados por 1.742 órgãos governamentais locais, faz com que o sistema jurídico seja uma parte significativamente complexa, inclusive com relação à privacidade de dados.[63]

Os tribunais do Japão são estruturados da seguinte forma: o sistema judiciário é dividido em oito Tribunais Superiores, tendo o Supremo Tribunal como sua principal corte constitucional. As decisões dos tribunais, em especial as do Supremo Tribunal, apesar de não vinculativas, possuem importância superior do que em alguns outros países de *Civil Law*. O Supremo Tribunal e cada tribunal inferior também são tribunais constitucionais. As decisões constitucionais relacionadas à liberdade de expressão e outras liberdades individuais afetam o desenvolvimento da privacidade de dados.[64]

Quanto às obrigações internacionais, o país é membro da OCDE e a legislação é influenciada pelas Diretrizes de privacidade da OCDE. No Japão, os tratados têm efeito direto como lei, mediante ratificação, sem exigir a implementação da legislação nacional. Assim, por exemplo, o Japão ratificou o Pacto Internacional sobre Direitos Civis e Políticos de 1966 em 1979, o que torna o Artigo 17 sobre privacidade parte da lei japonesa.[65]

Mais recentemente, conforme referido no capítulo 2, o Japão obteve decisão de adequação junto à União Europeia, abrangendo apenas o setor privado. Este fator permite que os dados pessoais circulem livremente entre as duas economias com base em fortes garantias de proteção de dados.[66]

3.2 Contexto de vigilância

Como em muitos países, existe uma estreita relação entre o desenvolvimento de sistemas de vigilância no Japão e o desenvolvimento de leis de proteção de dados. Importante salientar que, diferentemente do outro ordenamento analisado neste trabalho, o Japão, após a segunda guerra mundial, não experimentou uma revolta interna contra o governo autoritário e, portanto, as leis de proteção de dados nacionais não são vistas como parte do "pacote de liberdades", muitas vezes, característico de Estados pós-autoritários.[67] Portanto aqui o catalisador para a privacidade, elevado, no Japão, a uma questão de preocupação nacional, foi

---

[63] GREENLEAF, Graham. **Asian Data Privacy Laws: Trade & Human Rights Perspectives.** Oxford: Oxford University Press, 2014. E-book/Kindle Edition. p. 228 e 229.
[64] Ibid., p. 229.
[65] Ibid., p. 230.
[66] EUROPEAN COMMISSION. **European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows.** 2019. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421. Acesso em: 20 de jul. de 2021.
[67] GREENLEAF, op cit., p. 228.

a resistência pública e política à promulgação do Basic Resident Registers Act 1999.[68] Essa foi uma tentativa de converter o sistema baseado em papel (*Resident Basic Register System*), que rastreava os movimentos das pessoas entre as residências, em uma rede eletrônica nacional (*Juki-net*). O objetivo da *Juki-net* era combinar os bancos de dados de registro de residentes de 3.300 governos municipais e fornecer a todos os japoneses um número de identificação. A *Juki-net* é restrita por lei a apenas transmitir quatro dados pessoais (nome, sexo, data de nascimento e endereço). Contudo, o sistema não se desenvolveu como um modelo de identificação padrão no país, demonstrando uma maior resistência japonesa quanto ao vazamento de dados no ambiente digital, e, por consequência, à privacidade.[69]

A relação entre a valoração de normas sociais – por exemplo, o *giri*, conforme já mencionado – para a atual visão de privacidade pode ser vista como uma forte demonstração do senso japonês da proteção desta última. Em outras palavras, representa a migração quanto à dependência de normas sociais para o desenvolvimento de proteção legal de privacidade. O que destaca o forte senso japonês contemporâneo de privacidade.[70]

3.3 Contexto histórico e político de privacidade de dados

A legislação de proteção de dados no Japão, promulgada em 2003, era de difícil percepção, uma vez que poucos exemplos úteis da aplicação da mesma poderiam ser vislumbrados, até a reforma que entrou em vigor no ano de 2017. Como referido acima, anteriormente, a legislação nessa temática demonstrava as fraquezas dos princípios das leis de privacidade dos setores público e privado do Japão e da respectiva falta de aplicação, ambas agravadas pela carência de transparência. Entre os pontos fortes estavam a cobertura do setor público e a notificação exigida com relação à cobrança de terceiros. No entanto, tais princípios se mostravam como os mais limitados dentre as leis de privacidade de dados na Ásia, devido ao escopo restrito ao setor privado, exceções facilmente manipuladas para uso e limitações de divulgação, bem como pela falta de cláusulas de exclusão, assim como pela falta de provisões de informações sensíveis e, por fim, em função da falta de restrições à

---

[68] LAWSON, Carol. **Japan's New Privacy Act in Context.** Sydney: The University of New South Wales Law Journey (UNSW Law Journey), Volume 29(2), 2006. p. 97.

[69] TAKAMA, Gohsuke. **Lies and Secrets - Japan's National ID Network.** Anti National ID Japan, 2002. Disponível em: https://nationalid.hantai.jp/2002/08/lies_and_secret.html. Acesso em: 5 de out. de 2021.

[70] ADAMS, Andrew; MURATA, Kiyoshi; ORIOTO, Yohko. **The Japanese Sense of Information Privacy**. AI & Society, 24 (4), 2009. p. 12.

exportação de dados. Tais falhas em dar transparência ao sistema de fiscalização constituem uma grande deficiência, quando falamos de proteção de dados.[71]

Ponazecki[72] salientou em 2007 que: "não tem havido multas ou penalidades administrativas significativas ou sentenças judiciais decorrentes do descumprimento da Lei e das respectivas diretrizes" (tradução nossa). Assim, o principal risco para uma empresa privada que viola a Lei de Proteção de Informações Pessoais do Japão (LPIP-JP)[73] é geralmente o risco de danos à reputação, e não o risco de pagar multas pesadas ou ter que defender ações coletivas. Nessa direção, em 2011, Miyashita[74] evidenciou:

> As regras legais para os mecanismos de aplicação são muito particulares no Japão e diferem da forte aplicação da lei nos países europeus. No entanto, é extremamente importante entender que uma violação de dados no Japão significa a ruptura da confiança social e do relacionamento íntimo com os clientes. No Japão, o risco de perda de confiança social e reputação empresarial é considerado muito mais significativo do que pagar uma multa. Assim, as empresas geralmente seguem as diretrizes emanadas dos ministérios governamentais, e algumas também adotam suas próprias diretrizes, que vão ainda mais longe (tradução nossa).

A ruptura da confiança social é elemento fundamental para compreender a legislação japonesa, e a forma como a proteção de dados é abordada, uma vez que é elemento basilar do ordenamento jurídico japonês. Essas críticas sobre o conteúdo e a aplicação da lei de proteção de dados do Japão foram contempladas pelos legisladores japoneses nas reformas posteriores. Essas se deram, em parte, como resposta à revisão de 2013 das diretrizes de privacidade da OCDE, mas também como uma resposta às percepções internacionais sobre as fragilidades da lei japonesa e os obstáculos que poderia criar no futuro. Tais reformas tiveram como objetivos: a utilização de dados pessoais diante do advento do *big data*; a proteção da

---

[71] GREENLEAF, Graham. **Asian Data Privacy Laws: Trade & Human Rights Perspectives.** Oxford: Oxford University Press, 2014. E-book/Kindle Edition. p. 263.

[72] "[…] there have not been significant administrative fines or penalties or court judgments arising from failures to comply with the Law and the related guidelines […]". PONAZECKI, Jay; LEVISON, Daniel; MORRISON, So Toshihiro. **Japan: Personal information privacy update**. Washington: BNA International World Data Protection Report, 2007. p. 3. Disponível em: https://media2.mofo.com/documents/wdpr1207_privacy.pdf. Acesso em: 15 de nov. 2021.

[73] JAPAN. **Amended Act on the Protection of Personal Information (Lei nº 57 de 2003).** 2020. Disponível em: https://www.ppc.go.jp/files/pdf/APPI_english.pdf. Acesso em: 10 de out. de 2021.

[74] "The legal rules for enforcement mechanisms are very particular in Japan, and differ from the strong enforcement of the law in European countries. However, it is crucially important to understand that a data breach in Japan means the disruption of social trust and the intimate relationship with customers. In Japan, the risk of loss of social trust and business reputation is regarded as much more significant than paying a fine. Thus, businesses generally follow the guidelines issued by government ministries, and some also adopt their own guidelines which go even further." MIYASHI, Hiroshi. **The Evolving Concept of Data Privacy in Japanese Law**. Oxford: Oxford University Press, International Data Privacy Law, Volume 1, Issue 4, 2011. p. 233.

privacidade para atender às expectativas dos indivíduos; a criação de um ambiente em que as empresas japonesas possam utilizar dados pessoais, incluindo pessoas de fora do Japão, para criar novos negócios e serviços; revisões dos princípios de privacidade incluídos na LPIP-JP como um todo e o estabelecimento de uma autoridade supervisora independente.[75]

Como vimos anteriormente, a LPIP-JP foi aprovada originalmente em 2003 e foi atualizada várias vezes para exigir maior proteção de dados pessoais. Para se adaptar a fatores como a rápida evolução da tecnologia e dos padrões globais de proteção de dados pessoais, as emendas de 2017 exigiam que novas alterações fossem consideradas a cada três anos. Contudo, por mais que tais reformas tenham sido realizadas, nos últimos anos, o Japão sofreu uma série de violações de dados altamente prejudiciais, o que levou o governo japonês a reavaliar a atitude em relação à privacidade de dados e à cibersegurança.[76] De acordo com a revista "*The Economist",* o Japão "está atrás de outras economias avançadas" no que diz respeito à segurança cibernética. Muitos pequenos e médios negócios japoneses têm segurança mínima e muitas outras usam de tecnologia vulnerável; por exemplo, sistemas de computador que não oferecem mais *patches* de segurança.[77]

As emendas realizas em 2020, têm o conteúdo pautado em função de graves violações por parte de empresas japonesas. Por exemplo, em 2019, a rede de varejo japonesa Uniqlo revelou uma violação que comprometeu os dados de mais de 460.000 clientes.[78] Outro exemplo, uma empresa de tecnologia educacional, a Benesse, teve um vazamento de dados, no qual um funcionário de uma subsidiária roubou e vendeu os dados pessoais de cerca de 29 milhões de clientes.[79]

Assim, diante do atual cenário, é possível inferir que as empresas, de modo geral, possuem uma certa relutância ao observar as normas do LPIP-JP, muitas vezes, percebendo-as

---

[75] GREENLEAF, Graham. **Asian Data Privacy Laws: Trade & Human Rights Perspectives.** Oxford: Oxford University Press, 2014. E-book/Kindle Edition. p. 265, 266, 267 e 268.

[76] NUNN, Adam. **The New Japanese Privacy Law: What Businesses Need to Know.** 2020. Disponível em: https://auth0.com/blog/the-new-japanese-privacy-law-what-businesses-need-to-know/. Acesso em: 25 de out. de 2021.

[77] THE ECONOMIST. **Japan Inc's IT needs a security patch.** 2020. Disponível em: https://www.economist.com/business/2020/07/18/japan-incs-it-needs-a-security-patch. Acesso em: 6 de set. de 2021.

[78] THE JAPAN TIMES. **Uniqlo, GU brand's Fast Retailing says 460,000 online accounts were accessed in Japan hack.** 2019. Disponível em: https://www.japantimes.co.jp/news/2019/05/14/business/corporate-business/uniqlo-gu-brands-fast-retailing-says-460000-online-accounts-accessed-japan-hack/. Acesso em: 27 de set. de 2021.

[79] Id. **Benesse data thief gets 3½ years in prison, ¥3 million fine.** 2016. Disponível em: https://www.japantimes.co.jp/news/2016/03/29/national/crime-legal/benesse-data-thief-gets-3%C2%BD-years-prison-¥3-million-fine/. Acesso em: 27 de set. de 2021.

como uma burocracia desnecessária.[80] Contudo, tais emendas têm o potencial de corrigir deficiências graves na cultura de segurança cibernética japonesa, que, de outro modo, podem colocar em risco os dados de pessoas civis e jurídicas não apenas no país, mas até mesmo daqueles que estiverem fora dele.

3.4 Normas de privacidade de dados[81]

Primeiramente, é importante salientar que, devido ao escopo e dimensão do presente estudo, iremos privilegiar os seguintes pontos do ordenamento de proteção de dados no Japão: (i) estrutura geral das normas de proteção; (ii) Direito e Reponsabilidades (Controladores de dados pessoais, diretrizes gerais de comissão, pseudônima, informações anônimas, direitos e responsabilidade do processador, direitos dos titulares) e finalizar com a (iii) Notificação de dados e sanções. Esses elementos, em nosso entendimento, são aqueles que podemos considerar como os estruturantes do instituto da proteção de dados no país.

3.4.1 Estrutura geral das normas de proteção

Hoje, a legislação de proteção de dados japonesa se encontra basicamente fundada na LPIP-JP. A LPIP-JP foi sujeita a revisões substanciais com tempo, a mais recente, em 2020, foi promulgada, visando aumentar as obrigações das empresas, no sentido de serem transparentes e seguras com os dados pessoais de residentes japoneses, além de aumentarem as previsões penais para o vazamento de dados.[82]

A LPIP-JP se aplica a todos os Controladores de Dados Pessoais (CDP) no Japão, sejam pessoas físicas ou jurídicas, que lidam com informações pessoais no curso de negócios.[83] Segundo Hounslow, "[...] um "negócio" significa atividades que podem ser conduzidas repetidamente para um fim específico e são consideradas como um negócio de

---

[80] NUNN, Adam. **The New Japanese Privacy Law: What Businesses Need to Know.** 2020. Disponível em: https://auth0.com/blog/the-new-japanese-privacy-law-what-businesses-need-to-know/. Acesso em: 25 de out. de 2021.

[81] É importante frisar que, durante o desenvolvimento deste estudo, a maioria das informações sobre o instituo de proteção de dados no Japão foram encontradas no site da Comissão de Proteção de Informações Pessoais. Contudo, foi observada uma grande disparidade de informação entre as informações fornecidas pelo site em inglês, quando comparado à versão original em japonês. A versão em inglês dispõe de poucas diretrizes e de uma versão atualizada da LPIP-JP. Além disso, consta a informação de que as traduções não detêm caráter oficial.

[82] HOUNSLOW, Daniel. **Japan - Data Protection Overview.** OneTrust – Data Guidance, 2021. Disponível em: https://www.dataguidance.com/notes/japan-data-protection-overview. Acesso em: 6 de out. de 2021.

[83] JAPAN. **Amended Act on the Protection of Personal Information**. General Provisions; Purpose; Article 1, 2020. Disponível em: https://www.ppc.go.jp/files/pdf/APPI_english.pdf. Acesso em: 10 de out. de 2021.

acordo com as convenções sociais (tradução nossa).”[84] Desta forma, a incidência da lei se dá sobre o tratamento de informações pessoais por um CDP. Cabe destacar que, apesar do termo ter sido incluído nos debates realizados pelo comitê do governo, quando foi apresentado o esboço original da LPIP-JP (2000) – tendo, então, sido definido *tratamento* como “aquisição, retenção, uso, transferência e quaisquer outros atos que possam realizar trâmite de informações pessoais” –, esta definição não foi recepcionada pela LPIP-JP editada ou pelas diretrizes da Comissão de Proteção de Informações Pessoais do Japão (CPIP-JP).[85]

Segundo a LPIP-JP, o poder de exigir relatórios dos CDPs é delegado ao ministro que regula cada setor empresarial ou a ministro designado para este fim. Os Ministérios, assim, para cada um dos setores relevantes da economia, em conjunto com a CPIP-JP ou individualmente, emitem orientações, perguntas, respostas e comentários.[86]

À CPIP-JP, como regulador primário de acordo com a Lei, cabe:

a) garantir o tratamento adequado de informações pessoais e informações pessoais específicas, de modo a proteger os direitos e interesses dos indivíduos;[87]
b) atuar com poderes investigatórios, consultivos e de execução nos termos da LPIP-JP, incluindo o poder de investigar as atividades de um CDP, de um controlador de informações anonimizadas, de uma pessoa que lida com informações pessoais específicas e aconselhar e dar ordens contrárias a esses, se a violação dos direitos ou interesses materiais de um indivíduo for iminente;[88]
c) outorgar poderes de investigação a um ministro de jurisdição especifica;[89] e
d) prestar informações a reguladores de proteção de dados estrangeiros e, excepcionalmente, permitir que as informações sejam usadas para investigações criminais no exterior.[90]

Orientações emanadas da CPIP-JP detalham: (i) o escopo e o significado das regras; (ii) a terminologia adotada na LPIP-JP; e (iii) os exemplos de aplicação nos casos concretos. Diretrizes expressas devem ser observadas de forma cogente; a inobservância às diretrizes é

---

[84] “For this purpose, a 'business' means activities which can be conducted repeatedly for a particular purpose and are regarded as a business under social conventions; a business can be for profit or not.” HOUNSLOW, op cit.
[85] HOUNSLOW, Daniel. **Japan - Data Protection Overview.** OneTrust – Data Guidance, 2021. Disponível em: https://www.dataguidance.com/notes/japan-data-protection-overview. Acesso em: 6 de out. de 2021.
[86] JAPAN. **Amended Act on the Protection of Personal Information**. Obligations etc. of a Personal Information Handling Business Operator; Supervision; Article 44: 1, 2 e 3, 2020. Disponível em: https://www.ppc.go.jp/files/pdf/APPI_english.pdf. Acesso em: 10 de out. de 2021.
[87] Ibid., Duties; Article 60.
[88] Ibid., Jurisdictional Affairs; Article 61: (I, II, III, IV, V, VI, VII.)
[89] Ibid., Delegation of Authority; Article 44: (2).
[90] Ibid., Information Provision to the Foreign Enforcement Authorities; Article 78: 1, 2 e 3.

tratada como descumprimento da LPIP-JP.[91] É importante ressaltar que as diretrizes emitidas pela CPIP-JP compreendem os mais diversos setores, tais como: médico, trabalhista, das telecomunicações, financeiro, dentre outros, cuja ilustração completa fugiria ao escopo desta investigação. Alguns exemplos das diretrizes sobre a LPIP-JP, emitida pela CPIP-JP, incluem:[92]

a) Diretrizes Gerais;
b) Diretrizes para verificação e registro em transferências para terceiros;
c) Diretrizes para informações anônimas; e
d) Diretrizes sobre vazamentos de e violação de dados.

Diante dos elementos contemplados na proteção de dados no ordenamento japonês, entendemos como relevante destacar algumas definições que possuem mais relevância para o presente estudo. São elas:

Informações pessoais: Informações sobre pessoa que resida no Japão. Nessa categoria, incluem-se 'códigos de identificação pessoal', tais como: itens como caracteres, números, símbolos e/ou outros códigos para uso do computador que representam certas características físicas pessoais especificadas (como sequências de DNA, aparência facial, impressões digitais e palmares), e que são suficientes para identificar um indivíduo específico, bem como determinados números de identificação, como os de passaportes, carteiras de habilitação e cartões de residente e os números de identificação individual da previdência social.[93]

Dados pessoais: Informações pessoais contidas em um banco de dados.[94]

Dados sensíveis: informações pessoais relacionadas a questões como: raça, credo, religião, deficiência física ou mental, registros médicos, tratamento médico e farmacológico, prisão, detenção ou processo criminal (seja adulto ou jovem), ou vitimização criminal.[95]

Titular dos dados: o indivíduo que é o titular das informações pessoais.[96]

---

[91] HOUNSLOW, Daniel. **Japan - Data Protection Overview.** OneTrust – Data Guidance, 2021. Disponível em: https://www.dataguidance.com/notes/japan-data-protection-overview. Acesso em: 6 de out. de 2021.
[92] PERSONAL INFORMATION PROTECTION INFORMATION COMMISSION. **法令・ガイドライン等**. 2021. Disponível em: https://www.ppc.go.jp/personalinfo/legal/. Acesso em: 10 de out. de 2021.
[93] JAPAN. **Amended Act on the Protection of Personal Information**. General Provisions; Definition; Article 2: (1) - I e II, 2020. Disponível em: https://www.ppc.go.jp/files/pdf/APPI_english.pdf. Acesso em: 10 de out. de 2021.
[94] Ibid., Definition; Article 2: (6).
[95] Ibid., Definition; Article 2: (3).
[96] Ibid., Definition; Article 2: (8).

Informações processadas de forma pseudônima: Informações que foram processadas, a partir de informações pessoais, de forma que o titular dos dados não pode mais ser identificado.[97]

Controlador de informações processadas pseudonimamente: um operador de empresa que usa um banco de dados de informações processadas de forma pseudônima.[98]

Anonimização de dados: são informações sobre um indivíduo processadas pela exclusão de informações (ou substituindo-as por informações que não permitem a reversão para as informações originais), de forma que não possam ser usadas para identificar o indivíduo.[99]

Controlador de anonimização de dados: um operador de negócios que lida com informações anônimas, ou seja, um CDP que utiliza, nos negócios, base de dados que permite fácil acesso às informações específicas anonimizadas nele contidas.[100]

Assim, a partir das definições dos elementos centrais do instituto de proteção de dados japonês, discutiremos a aplicação de tais conceitos frente aos direitos e responsabilidades a eles vinculados.

3.4.2 Direitos e responsabilidades

A legislação japonesa determina que o CDP deve: (i) assegurar-se de coletar informações pessoais por meios oficiais e legais; (ii) notificar o titular dos dados quanto à finalidade da utilização, antes da coleta de informações pessoais[101]; e (iii) obter o consentimento do titular, antes de adquirir informações sensíveis.[102] Quanto à publicidade das informações, o CDP deve tornar acessíveis a cada titular: (i) o nome do CDP; (ii) a finalidade da utilização das informações pessoais coletadas; e (iii) o procedimento para o comitente solicitar a correção de dados pessoais, e mesmo onde reclamar do tratamento de dados pessoais pelo CDP.[103] Um CDP deve atuar apenas na medida necessária para atingir os

---

[97] JAPAN. **Amended Act on the Protection of Personal Information**. General Provisions; Definition; Article 2: (9), I e II, 2020. Disponível em: https://www.ppc.go.jp/files/pdf/APPI_english.pdf. Acesso em: 10 de out. de 2021.
[98] Ibid., Definition; Article 2: (10), 2020.
[99] Ibid., Definition; Article 2: (11), I e II.
[100] Ibid., Definition; Article 2: (12).
[101] Exceção a esta regra para a hipótese de que tenha sido publicado o objetivo da utilização com antecedência, de uma maneira prontamente acessível pelo titular.
[102] Ibid., Obligations of a Personal Information Handling Business Operator etc; Articles 15, 16 e 17.
[103] Ibid., Obligations of a Personal Information Handling Business Operator etc; Articles 18.

objetivos de utilização especificados pelo titular e deve envidar esforços para excluir os dados pessoais, quando esses não forem mais necessários para os fins de utilização.[104]

Agora, quanto ao gerenciamento e segurança de dados pessoais, um CDP deve tomar medidas razoáveis para manter as informações tão precisas e atualizadas quanto necessário, para atingir o propósito de utilização. Cumpre igualmente tomar todas as medidas de segurança necessárias para evitar a perda ou o acesso não autorizado aos dados pessoais, sendo necessário também que o CDP exerça supervisão necessária e apropriada sobre funcionários que lidam com os dados pessoais, ou quaisquer pessoas ou entidades delegadas que lidem com esses dados pessoais, de modo a garantir a segurança a tais informações.[105]

As medidas de segurança são ilustradas através das Diretrizes Gerais da CPIP-JP, para determinar exemplos de "alto nível de medidas de segurança", que são categorizadas em:[106]

a) Estabelecimento de princípios básicos e de regras internas na empresa;
b) Medidas de segurança organizacional, por exemplo, através de nomeação de uma pessoa responsável, definição da responsabilidade de cada pessoa, bem como definição do escopo dos dados tratados por cada membro da equipe;
c) Medidas de segurança de pessoal, por exemplo, educação e treinamento de pessoal e acordo de confidencialidade nas regras de trabalho;
d) Medidas de segurança física, por exemplo, controle de acesso de área por meio de cartões ou senhas, sistemas de prevenção contra roubo de dispositivo e prevenção de vazamento de dispositivos portáteis; e
e) Medidas de segurança tecnológica, como, controle de acesso ao sistema, prevenção de acesso não autorizado (instalação e atualização de software de segurança, criptografia, monitoramento de acesso) e revisão contínua de possíveis vulnerabilidades do sistema.

Além de tais medidas, as Diretrizes Gerais 'relaxam' os padrões de medidas de segurança para um operador de empresa de pequeno ou médio porte, que é definido como um CDP com 100 ou menos funcionários. Tais relaxamentos do padrão de segurança incluem as seguintes medidas:[107]

a) Estabelecimento de princípios básicos;

---

[104] JAPAN. **Amended Act on the Protection of Personal Information**. Obligations of a Personal Information Handling Business Operator etc; Article 19, 2020. Disponível em: https://www.ppc.go.jp/files/pdf/APPI_english.pdf. Acesso em: 10 de out. de 2021.
[105] Ibid., Assurance etc. about the Accuracy of Data Contents; Article 19 e 20.
[106] JAPANESE PERSONAL INFORMATION PROTECTION COMMISSIONN SECRETARIAT. **個人情報の保護に関する法律についてのガイドライン (通則編).** 3.3 (1, 2, 3 e 4) e 8 (1, 2, 3, 4, 5 e 6), 2016. Disponível em: https://www.ppc.go.jp/files/pdf/210101_guidlines01.pdf. Acesso em: 28 de out. de 2021.
[107] Ibid., 8 (1, 2, 3, 4, 5 e 6), 2016. Disponível em: https://www.ppc.go.jp/files/pdf/210101_guidlines01.pdf. Acesso em: 28 de out. de 2021.

b) Definição do processo básico de coleta, uso e armazenamento de dados pessoais para medidas de segurança organizacional;
c) Esclarecimento de quem é responsável pelo tratamento de dados pessoais e se mais de um membro da equipe lida com os dados;
d) Tratamento de acordo com o processo básico prescrito para a pessoa responsável pela verificação dos dados pessoais;
e) Permissão para verificação do processo de relatório de violação de dados com antecedência, para medidas de segurança física, medidas simplificadas (bloqueio de senha) e
f) Esclarecimento acerca de quais membros da equipe têm permissão para acessar os dispositivos, controlar o acesso do usuário, manter o software operacional dos dispositivos atualizado, apresentar software de segurança e definir senhas para abrir arquivos ao enviá-los por e-mail para medidas de segurança tecnológica.

Outra matéria disciplinada tanto pela CPPI quanto pela LPIP-JP são informações processadas de forma pseudônima. Nessa situação, um controlador de informações processadas de forma pseudônima está geralmente sujeito às mesmas obrigações de um CDP em relação ao gerenciamento e segurança das informações pessoais acima referidas, em conexão com informações processadas de forma pseudônima. No entanto, as obrigações de um CDP com relação às informações processadas de forma pseudônima são relaxadas em vários aspectos, por exemplo: o propósito de utilização pode ser alterado além do escopo razoavelmente relacionado ao propósito original de utilização, mesmo após a criação ou aquisição de informações processadas de forma pseudônima; as obrigações gerais de notificar o PPC e os titulares de uma violação de dados não são aplicáveis; assim como o direito do titular de acesso, correção ou pedido de cessação de uso não são aplicáveis.[108]

Um CDP que processa informações de pseudonimização não pode divulgar os métodos de pseudonimização das informações pessoais do titular. O controlador de informações processadas de forma pseudônima deve tomar medidas de segurança para evitar o vazamento de informações processadas de forma pseudônima e dados removidos, bem como supervisionar e controlar uma pessoa contratada para processar tais informações. Por último, o controlador de informações processadas de forma pseudônima não pode se referir a

[108] JAPAN. **Amended Act on the Protection of Personal Information**. Obligations of a Pseudonymously Processed Information Handling Business Operator etc.; Production etc. of Pseudonymously Processed Information; Article 35-2: (1, 2, 3, 4, 5, 6, 7, 8 e 9), 2016. Disponível em: https://www.ppc.go.jp/files/pdf/APPI_english.pdf. Acesso em: 10 de out. de 2021.

outras informações para re-identificar o titular relevante para as informações processadas de forma pseudônima.[109]

Da mesma forma, um CDP que cria informações anônimas não pode divulgar métodos de anonimato das informações pessoais dos titulares, os dados removidos no processo de anonimato ou qualquer processo usado para verificar o anonimato. Um destinatário de informações anônimas não pode tentar adquirir tais informações, seja do cedente ou de outra forma. Quando um CDP processa informações pessoais em informações anônimas, deve tornar público de maneira apropriada (por exemplo, através da internet) quais categorias de informações pessoais (por exemplo, idades, comportamento de compras e hábitos de viagem, etc.) estão incluídas nas informações anônimas, para que os titulares possam fazer consultas ao CDP.[110]

Agora, quanto aos direitos e responsabilidades do processador de dados, nem a LPIP-JP nem quaisquer regulamentos relacionados impõem quaisquer obrigações diretas a eles. No entanto, conforme evidenciado acima, a supervisão necessária e apropriada deve ser exercida por um CDP sobre quaisquer terceiros delegados para lidar com dados pessoais. Essas medidas de supervisão incluem a execução de acordos entre um CDP e um prestador de serviços, fornecendo medidas de segurança adequadas que devem ser tomadas pelo prestador de serviços, e o poder do CDP para instruir e investigar o prestador de serviços em relação ao tratamento dos dados pessoais confiados para isso. Assim, quando o controlador dos dados quiser realizar um acordo com um processador dos dados, são necessárias medidas de supervisão sobre quaisquer terceiros delegados para lidar com dados pessoais.

Quanto aos direitos dos titulares, esses, a qualquer momento, podem exigir o acesso a dados pessoais, obrigando o CDP a divulgar, em regra, por escrito e sem demora, os dados pessoais em posse desse. O acesso pode ser recusado se resultar em: lesão à vida ou segurança corporal, propriedade ou outros direitos e interesses do titular ou de terceiros; uma interferência material nas operações comerciais do CDP; ou uma violação de outras leis japonesas que proíbam a divulgação.[111]

Os titulares também têm o direito de revisar, corrigir, alterar ou excluir dados pessoais e solicitar a cessação do uso dos mesmos, se forem empregados para finalidade diferente da

---

[109] JAPAN. **Amended Act on the Protection of Personal Information**. Production etc. of Pseudonymously Processed Information; Article 35-2: (1, 2, 3, 4, 5, 6, 7, 8 e 9), 2016. Disponível em: https://www.ppc.go.jp/files/pdf/APPI_english.pdf. Acesso em: 10 de out. de 2021.

[110] Ibid., Obligations of an Anonymously Processed Information Handling Business Operator etc; Article 36, (1, 2, 3, 4, 5 e 6).

[111] JAPAN. **Amended Act on the Protection of Personal Information**. Obligations of a Personal Information Handling Business Operator etc; Article 27: (1, 2 e 3), 2016. Disponível em: https://www.ppc.go.jp/files/pdf/APPI_english.pdf. Acesso em: 10 de out. de 2021.

originalmente declarada, ou se foram adquiridos por fraude ou outros meios ilegais. Assim, se um titular solicitar que um CDP pare de usar dados pessoais daquele, o CDP deve fazê-lo, a menos que o pedido não seja razoável, ou a cessação seria cara ou de outra forma difícil, a exemplo da retirada de livros já distribuídos. Nesse caso, o CDP deve tomar medidas alternativas para proteger os direitos e interesses do titular. O CDP deve notificar o titular sem demora se a ação solicitada foi tomada e, se não for tomada, deve se esforçar para explicar os motivos. Um titular pode fazer valer direitos de exigir a revisão de dados pessoais por meio de ação civil, se tal pedido não for atendido dentro de duas semanas após ter sido feito.[112]

Por fim, conforme a legislação japonesa prevê, os titulares não têm nenhum dos direitos acima caso: os dados pessoais sejam apagados no prazo de seis meses após a coleta; ou se o titular ou outra pessoa vier a saber que existem tais dados pessoais mantidos pelo CDP que podem resultar em: lesão à vida ou segurança corporal, propriedade ou outros direitos e interesses do titular ou de terceiros; encorajar atos ilegais ou injustos; por em perigo a segurança nacional, prejudicar uma relação de confiança com um país estrangeiro ou organização internacional; prejudicar a negociação do país com um país estrangeiro ou organização internacional; ou apresentar um obstáculo à prevenção, repressão ou investigação de crimes ou prejudicar a segurança e a ordem públicas.[113]

3.4.2 Notificação de vazamento dos dados e sanções

As Diretrizes de Violação de Dados se limitam a estabelecer certos princípios para o tratamento de vazamentos, cabendo aos CDPs decidir quais ações específicas devem ser tomadas em relação aos fatos de cada caso. Portanto, tais diretrizes declaram que, em caso de vazamento, destruição ou dano às informações pessoais ou a probabilidade de qualquer um deles: é "desejável"[114] que o CDP afetado execute as seguintes etapas: (i) relatar o incidente dentro do CDP; (ii) tomar medidas para prevenir a ampliação/agravamento de qualquer dano (aos responsáveis ou terceiros afetados pelo incidente) em decorrência do incidente; (iii) conduzir uma investigação dos fatos relevantes e da causa do incidente; (iv) identificação das áreas afetadas nos servidores/sistemas do CDP e dos principais cujos dados foram afetados;

---

[112] Ibid., Obligations of a Personal Information Handling Business Operator etc; Article 29: (1, 2 e 3).

[113] JAPANESE PERSONAL INFORMATION PROTECTION COMMISSION SECRETARIAT. **個人情報の保護に関する法律についてのガイドライン (通則編).** 2-7 (1,2,3 e 4), 2016. Disponível em: https://www.ppc.go.jp/files/pdf/210101_guidlines01.pdf. Acesso em: 28 de out. de 2021.

[114] Não é incomum que as obrigações sob as leis e regulamentos japoneses sejam expressos como desejáveis ou semelhantes e, na ausência de fatores que determinem o contrário, a melhor prática seria cumprir a obrigação, a menos que haja um bom motivo para não fazê-lo. Além disso, quanto maior o dano que o não cumprimento pode causar, mais aconselhável se torna o cumprimento.

(v) planejar e implementar prontamente medidas para prevenir a recorrência do incidente ou outros incidentes que possam ocorrer devido ao incidente em questão; (vi) a menos que os dados vazados sejam criptografados em alto nível, notificar prontamente os titulares potencialmente afetados ou tornar os fatos do vazamento facilmente disponíveis para esses titulares (dependendo dos fatos de cada caso), com o objetivo de prevenir os titulares ou terceiros de incorrer em danos adicionais (por exemplo, para dar aos principais oportunidades para tomar medidas para evitar ou mitigar danos pelo uso de terceiros das informações vazadas); e (vii) anunciar publicamente os fatos relevantes e as medidas a serem tomadas para prevenir a recorrência do incidente.[115]

Assim, ao considerar se deve notificar os titulares afetados de uma violação de dados diretamente ou por meio de um aviso mais geral, os dois principais fatores a serem considerados por um CDP são a gravidade da perda e o dano que ela pode causar e a eficácia dos meios de notificação. Se uma perda puder causar danos graves, o curso prudente seria torná-la pública imediatamente e, em seguida, notificar as partes afetadas individualmente. Caso um CDP decida efetuar uma notificação geral, terá de avaliar a eficácia do meio de notificação provável; por exemplo, se a notificação for feita em um site, qual a probabilidade de as partes afetadas visitarem o site e por quanto tempo ele deve ser mantido ativo para notificar uma proporção apropriada dos principais afetados. Uma notificação, individual ou geral, deve incluir uma descrição da perda e as ações tomadas pelo CDP para mitigar efeitos, e seria aconselhável incluir um número de telefone ou endereço de e-mail que os titulares afetados possam utilizar para obter mais informações sobre a perda.

Até o momento, os CDPs que sofreram uma violação de dados muitas vezes ofereceram voluntariamente uma compensação às partes afetadas, tanto para prevenir quaisquer procedimentos quanto para manter boas relações públicas. Os pagamentos de compensação para um titular variaram de JPY 500 de *e-money* ou *vouchers*-presente, por meio de *vouchers*-presente de JPY 10.000, para pagamentos em dinheiro de JPY 35.000. Se uma parte afetada intentar uma ação perante um tribunal contra um CDP por violação de dados, qualquer decisão do tribunal seria provavelmente uma ordem contra o CDP para pagar indenização por violação de contrato ou teoria de delito civil. Salvo em casos como o uso não autorizado de dados de cartão de pagamento afetados ou a divulgação de informações confidenciais que afetam a vida pessoal de indivíduos, a quantidade de danos a que uma parte

---

[115] JAPANESE PERSONAL INFORMATION PROTECTION COMMISSION SECRETARIAT. **個人データの漏えい等の事案が発生した場合等の対応について**. 2017. Disponível em: https://www.ppc.go.jp/files/pdf/iinkaikokuzi01.pdf. Acesso em: 29 de out. de 2021.

afetada pode ter direito não é grande o suficiente para justificar o início do processo, uma vez que os custos do processo são tomados em consideração.[116]

3.5 Análise de caso concreto

Por fim, de modo a contextualizar a realidade e aplicação da proteção de dados no Japão, apresenta-se de grande relevância a análise de um precedente judicial sobre um caso concreto. No caso apresentado, podemos identificar claramente as características do instituto no ordenamento japones.

Como já citado acima, Benesse Holdings, Inc., um provedor de serviços de educação por correspondência, divulgou que sofreu um vazamento que afetou aproximadamente 29 milhões de clientes consistindo de crianças e dados pessoais dos respectivos pais. Tais dados incluíam nomes, endereços, números de telefone, sexo das crianças e datas de nascimento, bem como datas de entrega esperada do bebê de um número limitado de mães grávidas.[117] Em 2013 e 2014, um funcionário de uma empresa subcontratada pela subsidiária da Benesse, para processar os dados de clientes e se envolver no trabalho de processamento, passou a baixar ilegalmente os dados e vendê-los a corretores de listas de nomes. Tais dados, em última análise, haviam sido obtidos por outros prestadores de serviços, que enviaram e-mails de marketing direto para os pais e filhos afetados. A subsidiária implementou medidas de segurança, e como gesto de desculpas, a Benesse enviou um *voucher* de compra de JPY 500 para cada cliente identificado como afetado pelo incidente.

Diante desse caso, a decisão da Suprema Corte do Japão de 23 de outubro de 2017 anulou a decisão do tribunal inferior (Tribunal Superior de Osaka) de que o reclamante deveria ter estabelecido uma indenização além de um mero sentimento de desconforto ou ansiedade. Em vez disso, concluiu que a privacidade do reclamante foi infringida e reenviou o caso ao tribunal de primeira instância, para uma revisão mais aprofundada do dano moral devido à violação de privacidade. Assim, em 25 de março de 2020, o tribunal inferior julgou a Subsidiária e a Benesse como co-resposáveis por danos no valor de JPY 3.300 mais 5% de encargos atrasados por ano por indivíduo afetado.[118]

---

[116] HOUNSLOW, Daniel. **Japan - Data Protection Overview.** OneTrust – Data Guidance, 2021. Disponível em: https://www.dataguidance.com/notes/japan-data-protection-overview. Acesso em: 6 de out. de 2021.

[117] THE JAPAN TIMES. **Benesse data thief gets 3½ years in prison, ¥3 million fine.** The Japan Times Ltd, 2016. Disponível em: https://www.japantimes.co.jp/news/2016/03/29/national/crime-legal/benesse-data-thief-gets-3%C2%BD-years-prison-¥3-million-fine/. Acesso em: 27 de out. de 2021.

[118] HOUNSLOW, Daniel. **Japan - Data Protection Overview.** OneTrust – Data Guidance, 2021. Disponível em: https://www.dataguidance.com/notes/japan-data-protection-overview. Acesso em: 6 de out. de 2021.

4 COREIA DO SUL

A Coreia do Sul, país emergente do pós segunda guerra e fortemente desenvolvida em decorrência da guerra fria, conseguiu de forma exitosa migrar de um regime ditatorial para um calcado solidamente na democracia. Com o término gradual do regime militar não democrático, ocorrido especialmente a partir dos anos 80 do século passado, a República da Coreia estabeleceu, desde então, uma democracia multipartidária sólida e estável. Neste ambiente de estabilidade política e social, as conquistas no âmbito da proteção da privacidade foram, mais recentemente, sendo construídas, até mesmo por se imporem como contraponto às práticas do regime autoritário. Representam um elemento significativo da construção pós-autoritária de um estado liberal-democrático.[119]

4.1 Sistema legal

A história da estrutura legal Coreana surge a partir da Dinastia Joseon (1392 a 1897), com o estabelecimento dos principais elementos de organização do estado de direito. Após o fim desta dinastia, já durante o século 19, conceitos jurídicos originados no ocidente passaram a influenciar as normas sul-coreanas. Quando o Japão anexou o país, em 1910, houve a aceleração desta influencia, com os códigos japoneses se sobrepondo às leis da era Joseon, passando a ser a base fundamental da estrutura legal do país.[120]

Como consequência natural, considerando a adoção anterior, pelo Japão, de base legal europeia – especialmente os direitos alemão e francês -, a Coreia aceitou indiretamente a tradição jurídica ocidental. A história recente deste país fez com que houvesse a consolidação da base normativa japonesa, somada às influências ocidentais diretas, no caso, aquelas advindas dos Estados Unidos e da Europa, com influencias evidentes na Constituição de 1948 e sobre a separação de poderes. [121]

Tanto quanto no universo jurídico nipônico, a *civil law*, especialmente a de origem no direito germânico, permanece no ordenamento jurídico da Coréia do Sul, sendo a sua grande base estrutural das leis. A influência norte americana, por sua vez, também se encontra presente em muitos dos institutos legais sul-coreanos. O direito positivo é fortemente adotado

---

[119] GREENLEAF, Graham. **Asian Data Privacy Laws: Trade & Human Rights Perspectives.** Oxford: Oxford University Press, 2014. E-book/Kindle Edition. p. 124.
[120] Ibid., p. 125.
[121] KWON, Youngjoon. **Korea: Bridging the Gap between Korean Substance and Western Form.** Cambridge: Cambridge University Press, Law and Legal Institutions in Asia, E. Ann Black E Gary F. Bell, Eds., 2011. p. 151.

em alguns dos segmentos legais do país, sendo os estatutos fonte dominante do direito, complementados por decretos presidenciais ou ministeriais.[122]

O Poder Judiciário é estruturado por um Tribunal Constitucional, que é independente do Supremo Tribunal Federal, e que tem como uma das funções decidir a constitucionalidade da legislação. O Supremo Tribunal é a maior corte, acima de cinco Tribunais Superiores (de apelação), 18 Tribunais Distritais e vários tribunais especializados. Embora as decisões de tribunal não sejam formalmente consideradas fontes de direito, "as decisões da Suprema Corte funcionam como uma fonte de direito de fato".[123]

No que tange à proteção de dados, recentemente, em consonância com a conjuntura internacional, a República da Coreia passa atualmente pelos procedimentos para a efetivação da decisão de adequação com a União Europeia. Quando tais processos forem concluídos, os dados poderão fluir livremente entre a Coreia do Sul e União Europeia. Além disso, tal decisão aponta para forte grau de proteção de dados na Coreia dos Sul, conforme já referido no capítulo 2 acima.[124] Em síntese, todos os processamentos de informações pessoais realizados no país, estão abarcados na decisão de adequação. O que é divergente com relação à decisão do Japão, conforme já referido no capítulo anterior, que não abrangeu o setor público.[125]

4.2 Contexto de vigilância

A administração militar da Coreia do Sul, que durou até a década de 1990, adotava aparelho de vigilância estatal de extremo rigor. A Agência Central de Inteligência Coreana atuou até a presidência de Kim Young Sam, em 1992, quando foi reestruturada para reduzir as atividades de vigilância.[126] Apesar disto, ainda hoje em dia, a vigilância da população na Coreia do Sul permanece sendo realizada através do uso generalizado do número de registro de residente (NRR). Progressivamente, entretanto, o uso do número NRR, com a adoção de restrições a seu uso amplo, tem sido coibido. Esta evolução significa franco avanço neste

---

[122] GREENLEAF, Graham. **Asian Data Privacy Laws: Trade & Human Rights Perspectives.** Oxford: Oxford University Press, 2014. E-book/Kindle Edition. p. 125 e 126.

[123] KWON, Youngjoon. **Korea: Bridging the Gap between Korean Substance and Western Form.** Cambridge: Cambridge University Press, Law and Legal Institutions in Asia, E. Ann Black E Gary F. Bell, Eds., 2011. p. 166.

[124] EUROPEAN COMMISSION. **Data protection: European Commission launches the process towards adoption of the adequacy decision for the Republic of Korea.** 2021. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964. Acesso em: 27 de set. 2021

[125] GREENLEAF, Graham. **The Draft Korea Adequacy Decision: Submission to European Union Authorities.** Sydney: University of New South Wales Law Research Series, 2021. p. 2.

[126] ROBINSON, Michael Edson. **Korea's Twentieth-Century Odyssey: A Short History.** Honolulu: University of Hawaii Press, 2007. p. 171.

tema, especialmente considerando o histórico enraizado da cultura de vigilância encrustado na população sul-coreana. [127]

4.3 Contexto histórico e político de privacidade de dados

A Lei de Proteção de Informações Pessoais da Coreia do Sul (LPIP-CS), editada no ano de 2011, foi a primeira legislação de caráter abrangente, na qual foram incluídos sólidos conceitos de privacidade de dados e fiscalização quanto a seu uso. Uma Comissão de Proteção de Informações Pessoais independente de 15 membros foi instituída, o que representou forte sinalização à população sul-coreana quanto à construção da base de proteção de dados no país. A LPIP-CS é considerada atualmente pelos analistas como a legislação **"mais rígida do mundo"** sobre a matéria. Certamente, o fator catalizador deste processo remonta ao histórico autoritário dominante no país por diversas gerações. [128]

Nos dias atuais, considerado o país com melhor estrutura de internet do mundo, a proteção de dados é fator de contemporâneo destaque na sociedade sul-coreana. Mais de 80% da população do país é de usuários de internet. O uso de computadores pessoais está presente em praticamente todas as residências da nação, sendo quase todas as conexões de banda larga. A Coreia do Sul conta com a segunda maior conectividade de banda larga de fibra de alta velocidade entre os países da OCDE. O uso de internet móvel em telefones móveis é praticamente integral por parte da população.[129] Estes fatores acarretaram a adoção antecipada de algumas formas de serviços e regulamentação da internet na Coreia do Sul em primeiro lugar no mundo, fazendo com que o país se tornasse um importante terreno para o pioneirismo de questões ligadas à proteção de dados e ao uso da web.[130]

O desenvolvimento de leis de privacidade de dados na Coreia do Sul, portanto, ocorre no contexto de uma fase pós-autoritária, ocorrida no bojo de uma redemocratização e reestruturação da sociedade sul-coreana, sobre uma atual base tecnológica de vanguarda em âmbito mundial. A estrutura legislativa que lastreia o instituto é baseada em leis que têm

---

[127] PARK, Whon-il. **7. Republic of Korea.** 2008. p. 214 e 215. Disponível em: http://onepark.khu.ac.kr/Ch7_SKorea.pdf. Acesso em: 25 de set. de 2021.

[128] GREENLEAF, Graham; PARK, Whon-il Park. **Korea's New Act: Asia's Toughest Data Privacy Law.** 117 Privacy Laws & Business International Report, 2012. p. 1, 2, 3, 4, 5 e 6.

[129] DATA COMMONS. **Data Catalog WorldBank: South Korea.** 2021. Disponível em: https://datacommons.org/place/country/KOR?utm_medium=explore&mprop=count&popt=Person&cpv=isInternetUser%2CTrue&hl=en. Acesso em: 1 de set. de 2021.

[130] GREENLEAF, Graham. **Asian Data Privacy Laws: Trade & Human Rights Perspectives.** Oxford: Oxford University Press, 2014. E-book/Kindle Edition. p. 124.

menos de 20 anos, e foram forjadas sobre sólidos princípios originalmente depurados na União Europeia.

4.4 Normas de privacidade de dados

A exemplo da estrutura adotada acima, quando tratamos do tema da proteção de dados no Japão, considerando o escopo e a abrangência do presente estudo, manteremos os pontos de interesse no ordenamento de proteção de dados da Coreia do Sul em: (i) Estrutura geral das normas de proteção; (ii) direito e reponsabilidades (Controladores de dados pessoais, diretrizes gerais de comissão, pseudônima, informações anônimas, direitos e responsabilidade do processador, direitos dos titulares); e (iii) notificação de dados e sanções. A escolha por tais elementos se deveu ao fato de serem estes os principais aspectos que auxiliarão na compreensão da estrutura da proteção de dados neste país.

4.4.1 Estrutura geral das normas de proteção

Conforme antecipado acima, a coleta e o processamento de dados pessoais são regidos pela LPIP-CS de 2011. A LPIP-CS é aplicável a um manipulador de dados - ou seja, um órgão público, pessoa jurídica privada, organização ou indivíduo - que, por si ou por meio de terceiros, manipula dados pessoais para fazer uso ou realizar qualquer operação em um "arquivo de dados pessoais" no curso de atividades comerciais ou em relação a estas. O "arquivo de dados pessoais", por sua vez, significa um agrupamento de dados que são sistematicamente organizados de acordo com certas regras, para facilitar a pesquisa ou utilização de tais informações pessoais.[131]

Em linhas gerais, as leis de proteção de dados na Coreia do Sul estabelecem requisitos específicos e minuciosos no que se refere aos dados pessoais, ao longo do processo de tratamento destes. Os requisitos de notificação prévia e as sanções relativamente pesadas, prescritos na legislação sul-coreana, são considerados, como já mencionado anteriormente aqui, como um dos conjuntos normativos de proteção de dados mais rígidos do mundo. O

[131] KANG, Minchae. **South Korea - Data Protection Overview.** OneTrust – Data Guidance, 2021. Disponível em: https://www.dataguidance.com/notes/south-korea-data-protection-overview. Acesso em: 6 de out. de 2021.

conjunto de proteção de dados da República da Coreia consistem em uma lei geral (LPIP-CS) e várias leis especiais relativas a certos setores específicos da indústria.[132]

Recentemente, em 4 de fevereiro de 2020, foram aprovadas diversas emendas ao texto da LPIP-CS, que passaram a viger a partir de 5 de agosto de 2020. Estas emendas incluíram, entre outras, revisões às definições de processamento de pseudônimos e anônimos, bem como requisitos, restrições e penalidades associados a estes itens, bem como medidas para centralizar os serviços de proteção de informações pessoais na Comissão de Proteção de Informações Pessoais da Coreia do Sul (CPIP-CS).[133]

Além da lei geral, um conjunto de leis especiais regulam o tratamento de dados pessoais em determinados setores específicos da economia; por exemplo, a Lei de Uso e Proteção de Informações de Crédito (LUPIC).[134] Já o processamento de dados pessoais por Provedores de Serviços de Informação e Comunicação (PSICs) e destinatários de tais informações, que era originalmente regido pela Lei de Promoção da Informação e da Utilização da Rede de Comunicação e Proteção da Informação (RCPI), de 2001, atualmente é regido pela LPIP-CS, a partir da exclusão de dispositivos da RCPI e transferência para a LPIP-CS, a contar de 5 de agosto de 2020. Essas disposições estão agora incluídas na LPIP-CS como um novo capítulo, Disposições Especiais para os PSICs.[135] Estes movimentos legislativos denotam a atenção do legislador sul-coreano ao instituto e ao constante aperfeiçoamento da atividade de tratamento de dados no país.

Apesar de ter ocorrido a transferência dos principais regramentos da RCPI para a LPIP-CS, como as disposições especiais para os PSICs, foram mantidas a vigência da RCPI para questões de processamento de dados por PSICs para fornecedores comerciais de serviços de informação, incluindo aqueles fornecidos através da utilização de um serviço de telecomunicações. Ou seja, os serviços de internet e fornecedores de serviços *online*, incluindo fornecedores de conteúdos e fornecedores de aplicações, e prestadores de serviços de telecomunicações, permaneceram sob o regime estabelecido na RCPI.[136]

Já a LUPIC, norma com foco na área de proteção de informações no âmbito do crédito, regulamenta as atividades: (i) das empresas de informações de crédito (ou seja,

---

[132] KANG, Minchae. **South Korea - Data Protection Overview.** OneTrust – Data Guidance, 2021. Disponível em: https://www.dataguidance.com/notes/south-korea-data-protection-overview. Acesso em: 6 de out. de 2021.

[133] KANG, H Chris; KIM, Hee Sun. **Recent major amendments to three South Korean data privacy laws and their implications.** International Bar Association, 2020. Disponível em https://www.ibanet.org/article/0D5FD702-179C-42A1-B37D-45D12F4556DA. Acesso em: 1 de out. de 2021.

[134] SOUTH KOREA. **Use and Protection of Credit Information Act.** 2001. Acesso em: https://www.privacy.go.kr/eng/laws_view.do?nttId=8188&imgNo=2. Disponível em: 10 de nov. de 2021.

[135] KANG, Minchae. op cit.

[136] Ibid.

agências de crédito para pessoas físicas, agências de crédito para empresas individuais, agências de crédito para empresas, empresas de investigação de crédito); (ii) das empresas de autogestão de informações de crédito, envolvidas no negócio de fornecer informações de crédito para sujeitos de informações de crédito; (iii) agências de coleta de informações de crédito que gerenciam/utilizam as informações de crédito que coletaram; (iv) agências de cobrança de dívidas; e (v) usuários e provedores de informações de crédito (ou seja, pessoas que fornecem a terceiros informações de crédito, obtidas ou geradas em conexão com transações comerciais, como transações financeiras, com clientes, ou pessoas que recebem por terceiros tais informações de crédito, para serem usadas em negócios, por exemplo, um banco ou uma empresa de cartão de crédito).[137]

Portanto, mesmo havendo legislação geral, no caso a LPIP-CS, as leis especiais regulamentam o tratamento de dados em determinados segmentos, "de forma especializada". Assim, se uma disposição de uma lei especial for considerada aplicável a uma entidade, ela deve estar em conformidade com a disposição da lei especial (por exemplo, a LUPIC) antes da LPIP-CS.[138] Para os PSICs, mesmo nos casos em que a LPIP-CS seja aplicável, as Disposições Especiais para os PSICs se sobrepõem prioritariamente aos regramentos gerais.[139]

Desde o início da normatização de proteção de dados na Coreia do Sul, foram emitidas diversas diretrizes com detalhamentos sobre o tema, tais como: (i) um guia para a interpretação das leis e regulamentos de proteção de dados, emitido pelo Ministério do Interior e Segurança; (ii) parâmetros para a Desidentificação de Dados Pessoais, emitidas por um anúncio governamental feito sob a liderança conjunta do Escritório de Coordenação de Políticas Governamentais, a Comissão de Comunicações da Coreia (CCC), a Comissão de Serviços Financeiros (CSF), o Ministério da Ciência e TIC e o Ministério da Saúde e Bem-Estar; (iii) diretrizes para pseudonimização de dados pessoais, emitidas pela CPIP-CS; e (iv) um manual sobre pseudonimização e anonimato de dados pessoais no setor financeiro. Embora essas diretrizes não tenham efeito legal vinculante, elas podem, entretanto, servir como materiais de referência úteis sobre como as leis e regulamentos, em suas aplicações em concreto.[140]

---

[137] SOUTH KOREA. **Use and Protection of Credit Information Act.** 2001. Acesso em: https://www.privacy.go.kr/eng/laws_view.do?nttId=8188&imgNo=2. Disponível em: 10 de nov. de 2021.

[138] Ibid., Article 4 (Policy for Promotion of Information and Communications Network Utilization and Data Protection, etc.).

[139] KANG, Minchae. **South Korea - Data Protection Overview.** OneTrust – Data Guidance, 2021. Disponível em: https://www.dataguidance.com/notes/south-korea-data-protection-overview. Acesso em: 6 de out. de 2021.

[140] KOREA LAW INFORMATION CENTER. **LAW.** 2021. Disponível em: https://www.law.go.kr/LSW/eng/engLsSc.do?menuId=2&section=lawNm&query=Credit%20Information&x=13&y=26#liBgcolor29. Acesso em: em 27 de set. de 2021.

As principais autoridades de proteção de dados na Coreia do Sul são[141]:

a) a CPIP-CS, como órgão responsável por fazer cumprir a LPIP-CS, abordando questões relativas a interpretações formais, impondo multas administrativas, penalidades adicionais, ordens corretivas e outras sanções administrativas; além disto, cabe à CPIP-CS, ainda, a definição da política de proteção de dados, a avaliação e a promulgação/alteração de leis e medidas administrativas relacionadas à proteção de informações pessoais;
b) a CCC, responsável por fazer cumprir a RCPI, abordando questões relativas a interpretações formais, imposição de multas administrativas, penalidades adicionais, ordens corretivas e outras sanções administrativas no âmbito deste regramento;
c) a Agência de Internet e Segurança da Coreia, com a principal função de executar tarefas que lhe sejam delegadas pela CCC e pela CPIP-CS; e
d) a CSF, com a atribuições de fazer cumprir a LUPIC, e abordar questões relativas a interpretações formais deste regramento.

Por fim, a LPIP-CS estabelece as seguintes definições básicas na aplicação do instituto do país:

Dados pessoais: são sempre dados relativos a uma pessoa física viva que: (i) seja identificável como determinado indivíduo pelo nome completo, NRR, imagem ou elemento semelhante; (ii) mesmo se por si só não seja identificável, possa ser determinado o indivíduo, a partir da combinação com outras informações; ou (iii) são informações previstas nos itens (i) ou (ii) acima que são pseudonimizadas e, portanto, tornam-se incapazes de acarretar a identificação de um determinado indivíduo sem o uso ou combinação de informações adicionais para restauração ao estado original.[142]

Coleta de dados: é o manuseio de dados pessoais envolvendo a coleta, a geração, a gravação, o armazenamento, a retenção, o processamento, a edição, a pesquisa, a saída, a retificação, a restauração, o uso, o fornecimento, a divulgação ou destruição de dados pessoais ou qualquer outra ação semelhante a qualquer uma destas. [143]

Dados sensíveis: os dados sensíveis são definidos como informações pessoais relacionadas à ideologia, religião, associação a sindicatos ou partidos políticos de um indivíduo, opiniões políticas, saúde, orientação sexual e outras informações pessoais que

---

[141] KANG, Minchae. **South Korea - Data Protection Overview.** OneTrust – Data Guidance, 2021. Disponível em: https://www.dataguidance.com/notes/south-korea-data-protection-overview. Acesso em: 6 de out. de 2021.
[142] SOUTH KOREA. **PERSONAL INFORMATION PROTECTION ACT**. General Provisions; Article 2, (1), 2020. Disponível em: https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=3. Acesso em 25 de set. de 2021.
[143] Ibid., General Provisions; Article 2, (2).

podem causar uma violação material da privacidade, incluindo informações genéticas, registros criminais, informações sobre as características físicas, fisiológicas e comportamentais de um indivíduo - geradas por determinados meios técnicos com o objetivo de identificar um indivíduo específico - e dados raciais/étnicos.[144]

Controlador de dados: O conceito de manipulador de dados, ou controlador de informações pessoais, na LPIP-CS é semelhante ao conceito de controlador de dados no Regulamento Geral de Proteção de Dados (Regulamento (UE) 2016/679) (RGPD). Especificamente, a LPIP-CS define um manipulador de dados como 'uma instituição pública, pessoa jurídica, organização, indivíduo, que, por si ou por meio de terceiros, processa, ou seja, coleta, gera, conecta, bloqueia, registra, armazena, retém, processa, edita, pesquisa, produz, corrige, restaura, usa, fornece, divulga, destrói ou de outra forma manipula dados pessoais para administrar arquivos de dados pessoais para fins oficiais ou comerciais.[145]

Processador de dados: são pessoas que, contratadas pelos manipuladores (controladores) de dados, processarão – de forma terceirizada – os dados pessoais e informações pessoais controlados pelo manipulador detentor dos mesmos; é relevante destacar que, segundo a LPIP-CS, o conceito de manipulador de dados inclui autoridades de proteção de dados que processam dados.[146]

4.4.2 Direitos e responsabilidades

Os CDPs de dados devem atentar para uma gama ampla de observâncias dos regramentos emitidos pela LPIP-CS. Devem, no tratamento de dados pessoais, adotar procedimentos visando a minimização dos riscos qualquer possível violação da privacidade dos titulares. Sempre que possível, a anonimização dos dados pessoais deve ser adotada. Caso não seja possível anonimizá-los, a pseudonimização deve ser implementada antes do processamento. No caso especifico dos manipuladores de dados, estes devem manter a segurança dos dados pessoais, levando em consideração a probabilidade e o risco de violação da privacidade. Esta probabilidade e nível de risco podem variar dependendo de vários fatores, tais como, exemplificativamente, os tipos e métodos de tratamento de dados pessoais. Cabe aos manipuladores de dados, também, a obrigação de adotar todas as medidas técnicas,

---

[144] SOUTH KOREA. **PERSONAL INFORMATION PROTECTION ACT**. Limitation to Processing of Personal Information; Article 23., 2020. Disponível em: https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=3. Acesso em: 25 de set. de 2021.
[145] Ibid., Definitions; Article 2, (5).
[146] Ibid., Supervision of Personal Information Handlers, Article 28.

administrativas e físicas necessárias para garantir a segurança dos dados pessoais. Essas medidas incluem, entre outras coisas, o estabelecimento de regras internas para a administração adequada de dados pessoais e a manutenção de registros de acesso para evitar que os dados pessoais sejam perdidos, roubados, vazados, fabricados ou destruídos.[147]

Os manipuladores de dados também devem expressamente avisar aos titulares quando processarem dados pessoais. O consentimento expresso é geralmente necessário antes da coleta/uso/fornecimento de dados pessoais. O consentimento para uma provisão deve ser obtido separadamente do consentimento para a coleta e uso de dados pessoais. Além disso, o consentimento para o processamento de dados de identificação específicos - ou seja, NRRs, números de passaporte, números de carteira de motorista e números de registro de estrangeiro e dados sensíveis - devem ser obtidos separadamente uns dos outros e de qualquer outro consentimento. Os dados pessoais não devem ser usados fora dos propósitos consentidos.[148]

As Emendas editadas em 2020 excetuaram algumas hipóteses à regra geral de necessidade de consentimento do titular de dados. Os dados pessoais podem ser usados/fornecidos sem o consentimento do titular dos dados, dentro de algum escopo razoavelmente relacionado ao objetivo original da coleta. Nesta hipótese, desde que tal uso/fornecimento de informações pessoais poderia ter sido previsto, à luz das circunstâncias que o cercam, em situação de práticas de manuseio habituais, e não havendo qualquer desvantagem para o titular dos dados, a falta de consentimento pode ser aceita.[149]

Quanto aos direitos e responsabilidades do processador de dados, eles estarão, em geral, sujeitos às mesmas obrigações legais aplicáveis aos manipuladores de dados. No caso de violação da LPIP-CS por um processador de dados, ou seja, um provedor de serviços terceirizado, o processador de dados será considerado um preposto do manipulador de dados e este terá responsabilidade indireta.[150] O CDP, ao terceirizar o processamento de dados pessoais para um processador de dados, deve contratar por escrito, estabelecendo no mínimo: (i) os termos que proíbem um processador de dados de processar dados pessoais para qualquer fim, que não seja para o desempenho das tarefas terceirizadas; (ii) as salvaguardas técnicas e administrativas implementadas, para a proteção de dados pessoais; e (iii) quaisquer outras

---

[147] SOUTH KOREA. **PERSONAL INFORMATION PROTECTION ACT**. Principles for Protecting Personal Information; Art. 3, (4, 6, 7 e 8)., 2020. Disponível em: https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=3. Acesso em: 25 de set. de 2021.

[148] Ibid., Safeguard of Persona Information; Article 29.

[149] KANG, Minchae. **South Korea - Data Protection Overview.** OneTrust – Data Guidance, 2021. Disponível em: https://www.dataguidance.com/notes/south-korea-data-protection-overview. Acesso em: 6 de out. de 2021.

[150] SOUTH KOREA, op cit., Designation of Privacy Officers; Article 31.

questões definidas pelo Decreto de Execução da LPIP-CS, visando a administração segura de dados pessoais.[151]

Aos titulares de dados, o manipulador sempre deve garantir que os dados pessoais sejam precisos, completos e atualizados na medida necessária para atingir os objetivos de manuseio, e os titulares dos dados podem exercer os direitos de acesso, correção, suspensão de uso e remoção de dados pessoais. Para estes efeitos, a LPIP-CS também dispõe de regras processuais prescritivas que asseguram o exercício dos referidos direitos pelos titulares dos dados.[152]

Finalmente, à luz da LPIP-CS, todos os manipuladores de dados devem indicar funcionários qualificados para atuarem como agentes de privacidade e assumir o controle de todos os aspectos da operação do tratamento de dados pessoais. Especificamente, os manipuladores de dados, excluindo instituições públicas, devem nomear uma pessoa que atue como oficial de privacidade. Esta pessoa deverá ser o proprietário ou o diretor representante da empresa; não havendo diretores passíveis de assunção da função, então o chefe do departamento responsável pelo tratamento de dados pessoais.[153] No caso de instituições públicas, o oficial de privacidade deve ser um funcionário público que atenda a certos requisitos prescritos pela legislação.[154]

4.4.2 Notificação de vazamento dos dados e sanções

Segundo a LPIP-CS, ocorrendo um vazamento de dados, o manipulador destes dados deve notificar os titulares afetados por este fato, imediatamente a partir do momento que toma conhecimento da ocorrência de uma violação de dados pessoais controlados por ele. Além disso, ocorrendo violação de dados envolvendo 1.000 ou mais titulares de dados, o manipulador destes dados deve, além de remeter avisos individuais aos titulares, relatar a violação à CPIP-CS ou a uma instituição especializada designada pela LPIP-CS. Deve, ainda, também divulgar as informações sobre o vazamento em *homepage* na internet, ou em locais

---

[151] SOUTH KOREA. **PERSONAL INFORMATION PROTECTION ACT.** Limitation to Personal Information Processing Subsequent to Outsourcing of Work; Article 26, 2020. Disponível em: https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=3. Acesso em: 25 de set. de 2021.

[152] Ibid., Principles for Protecting Personal Information; Article 3.

[153] Ibid., Supervision of Personal Information Handlers; Article 28.

[154] KANG, Minchae. **South Korea - Data Protection Overview.** OneTrust – Data Guidance, 2021. Disponível em: https://www.dataguidance.com/notes/south-korea-data-protection-overview. Acesso em: 6 de out. de 2021.

visíveis do estabelecimento comercial desse, se não operar uma *homepage* na internet. Esta divulgação deve ser feita durante, pelo menos, sete dias.[155]

Na mesma linha das obrigações dos CDPs, os PSICs, assim como os destinatários dos dados pessoais fornecidos pelos PSICs, estão sujeitos às Disposições Especiais sobre os PSICs. Assim, ocorrendo vazamento a partir da manipulação de dados realizada por estas entidades, a notificação deve ser fornecida aos titulares dos dados e à CPIP-CS ou à instituição especializada regulamentada, sem demora, no prazo de até 24 horas após a ocorrência de uma violação de dados.[156]

Quanto às possibilidades de sanções, os reguladores (CPIP-CS, a CCC e a CSF) podem impor várias sanções administrativas, como ordens corretivas, multas administrativas e sobretaxas penais por violações das respectivas leis e regulamentos. Os promotores públicos, também podem investigar quaisquer violações que igualmente sejam passíveis de punição criminal; além de imputar responsabilidade civil por quaisquer titulares de dados que sofram danos, como resultado de tais violações.[157]

Outro elemento importante de ser salientado é que o ordenamento sul-coreano fornece aos indivíduos vários mecanismos para fazer cumprir efetivamente os respectivos direitos e obter reparação (judicial). Isso inclui as obrigações dos CDPs e a operação de instituições corretivas especializadas - o Centro de Atendimento à Privacidade operado pela KISA e os Comitês de Mediação de Disputas. Além disso, existem disposições para uma mediação de conflitos coletivos, com ações coletivas daí resultantes. Finalmente, existem disposições na LPIP-CS para ações corretivas a serem tomadas perante um Tribunal, que podem resultar em compensação de US$ 3.000/titular, sem necessidade de provar o dano real. Além de opções de baixo custo e fácil acesso, por exemplo, o Call Center de Privacidade, realizando mediação coletiva, por meio de adoção de medidas administrativas perante o PIPC, ou até mesmo vias judiciais, inclusive com a possibilidade de obter indenização por perdas e danos.[158]

---

[155] SOUTH KOREA. **PERSONAL INFORMATION PROTECTION ACT.** Data Breach Notification; Article 34., 2020. Disponível em: https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=3. Acesso em 25 de set. de 2021.

[156] Ibid., Special Cases on the Notification and Reporting on the Divulgence of Personal Information; Art. 39-4, 2020.

[157] Ibid., Penalty Provisions, Articles 70, 71, 72, 73, 74, 74-2, 75 e 76

[158] GREENLEAF, Graham. **The Draft Korea Adequacy Decision: Submission to European Union Authorities.** Sydney: University of New South Wales Law Research Series, 2021. p. 11.

4.5 Análise de caso concreto

Sendo uma jurisdição de *civil law*, a principal fonte de autoridade legal da Coreia do Sul é a legislação, ao contrário da jurisprudência em jurisdições de direito consuetudinário e, em particular, as codificações na Constituição da República da Coreia e os estatutos promulgados pelo Governo da República da Coreia ou a Assembleia Nacional. No entanto, várias decisões judiciais importantes foram emitidas recentemente que podem servir como referências úteis sobre como as leis e regulamentos de proteção de dados podem ser interpretados na prática.

Na Decisão do Supremo Tribunal[159], decidida em 7 de abril de 2017, o Supremo Tribunal da Coreia invalidou o consentimento obtido dos titulares dos dados porque o réu havia coletado informações pessoais em circunstâncias que dificultaram aos titulares dos dados compreenderem claramente o que haviam consentido, ainda que o consentimento lhes tenha prestado cumpriu as formalidades previstas na lei, ou seja, o aviso foi prestado em fonte de 1mm.[160]

Além disso, na Decisão[161], julgado em 3 de maio de 2019, o Tribunal Superior determinou que o Centro de Informações Farmacêuticas da Coreia fornecesse informações pessoais sensíveis, ou seja, dados de prescrição de pacientes para terceiros, sem consentimento constituiu violação da LPIP-CS. Ao mesmo tempo, o Tribunal Superior observou que se as informações pessoais foram submetidas a medidas de desidentificação adequadas, como criptografia, o que torna impossível identificar indivíduos específicos, então o fornecimento de tais dados desidentificados a terceiros sem o consentimento dos titulares dos dados não deve ser considerada uma violação da LPIP-CS.[162]

---

[159] Supremo Tribunal da Coreia do Sul. **Decissão 2016 Do13263.** 2016.
[160] KANG, Minchae. **South Korea - Data Protection Overview.** OneTrust – Data Guidance, 2021. Disponível em: https://www.dataguidance.com/notes/south-korea-data-protection-overview. Acesso em: 6 de out. de 2021.
[161] Tribunal Superior de Seul. **Decisão: 2017Na2074963/2017Na2074970.** 2017.
[162] KANG, op cit.

5 ANÁLISE COMPARATIVA ENTRE O SISTEMA DE PROTEÇÃO DE DADOS DO JAPÃO E DA COREIA DO SUL

Após a devida contextualização e exposição do instituto da proteção de dados, tanto no Japão quanto na Coreia do Sul, analisaremos comparativamente os dois ordenamentos, visando identificar quais as principais diferenças entre ambos. Buscaremos, ainda, estabelecer se as distinções constatadas influenciaram ou influenciarão na decisão de adequação da União Europeia.

5.1 Normas de proteção de dados no Japão e na Coreia do Sul

Tendo em vista o que antes referimos, no sentido de que ambos os países possuem legislação geral sobre o tema (LPIP-JP e LPIP-CS), compararemos essas normas, buscando verificar as características individuais e as diferenças. Identificadas as peculiaridades diversas entre ambas, analítica e comparativamente buscaremos apontar a forma como cada uma das nações abordou o instituto da proteção de dados e quais evidências ressaltam as principais diferenças entre elas.

5.1.1 Estrutura geral das normas de proteção de dados

Inicialmente, as distinções se mostram perceptíveis na forma como as normas de proteção de dados estão estruturadas. Enquanto a legislação de proteção de dados japonesa se encontra basicamente fundada na LPIP-JP e diretrizes nacionais, a Coreia do Sul optou por, além de adotar uma lei geral (LPIP-CS) e diretrizes próprias do país, promulgar diversas leis de proteção de dados especiais relativas a certos setores específicos da economia.[163] Uma das principais características presentes nesse instituto, no Japão, se encontra na forma como a LPIP-JP delega o poder de exigir relatórios dos CDPs aos ministros de um setor especificamente designado. [164]

---

[163] KANG, Minchae. **South Korea - Data Protection Overview.** OneTrust – Data Guidance, 2021. Disponível em: https://www.dataguidance.com/notes/south-korea-data-protection-overview. Acesso em 6 de Outubro de 2021.

[164] JAPAN. **Amended Act on the Protection of Personal Information**. Obligations etc. of a Personal Information Handling Business Operator; Supervision; Article 44: 1, 2 e 3, 2020. Disponível em: https://www.ppc.go.jp/files/pdf/APPI_english.pdf. Acesso em: 10 de out. de 2021.

Quanto as revisões relativas ao ordenamento, ambos os países receberam reformas substanciais ao longo do tempo. No Japão, em 2020, um projeto de lei foi aprovado visando aumentar as obrigações das empresas em serem transparentes e seguras com os dados pessoais de residentes japoneses ou de qualquer um que corra risco de incorrer em penalidades criminais.[165] Por outro lado, as emendas sul-coreanas incluíram definições revisadas para processamento de pseudônimos e anônimos (elemento já abarcado e bem detalhado pelo ordenamento japonês), bem como requisitos, restrições e penalidades (elemento não tão definido pela CPIP-CS e as respectivas diretrizes).[166]

Quanto às diretrizes emitidas por ambos os países, é interessante frisar que, embora as diretrizes vinculadas a LIPI-CS não tenham efeito legal vinculante, elas podem, no entanto, servir como materiais de referência úteis sobre a interpretação prática das leis e regulamentos.[167] Enquanto isso, as diretrizes japonesas deixam claro que a violação de uma diretriz expressa como uma obrigação, e não como uma recomendação, é considerada uma violação da LPIP-JP.[168] Conforme evidenciado no capítulo 3, as diretrizes japonesas raramente expressam alguma obrigação, e isso se configura como um questionamento quanto à compatibilidade da adequação do país com a UE.

Outro ponto de divergência se encontra nas principais definições apresentadas por cada um dos institutos. Enquanto o instituto de proteção de dados, do Japão, abarca uma gama de conceitos maior do que os presentes na Coreia do Sul, algumas questões fundamentais devem ser levantadas: (i) ausência da definição para Controlador de Dados ou Processador de Dados, por parte da LPIP-JP e (ii) um detalhamento maior por parte dos conceitos apresentados na LPIP-CS. Por conseguinte, o ordenamento coreano se configura, aparentemente, mais simples; contudo, mais complexo em definições, e, conforme observaremos no decorrer desta análise comparativa, mais rígido também. Em contrapartida, o ordenamento japonês determina uma enorme lista de definições; já a LPIP-CS tem uma espinha dorsal mais sólida dos respectivos elementos basilares. Exemplo de tais divergências, quanto à estruturação, é evidenciado na previsão legal de dados pessoais por parte da LPIP-

---

[165] HOUNSLOW, Daniel. **Japan - Data Protection Overview.** OneTrust – Data Guidance, 2021. Disponível em: https://www.dataguidance.com/notes/japan-data-protection-overview. Acesso em: 6 de out. de 2021.

[166] KANG, Minchae. **South Korea - Data Protection Overview.** OneTrust – Data Guidance, 2021. Disponível em: https://www.dataguidance.com/notes/south-korea-data-protection-overview. Acesso em: 6 de out. de 2021.

[167] SOUTH KOREA. **Personal Data and Protection Law in South Korea: Laws & Policies.** 2021. Disponível em: https://www.privacy.go.kr/eng/laws_policies_list.do. Acesso em: 27 de set. de 2021.

[168] JAPANESE PERSONAL INFORMATION PROTECTION COMMISSION SECRETARIAT. **Report by the Personal Information Protection Commission Secretariat: Anonymously Processed Information.** 2017. Disponível em: https://www.ppc.go.jp/files/pdf/The_PPC_Secretariat_Report_on_Anonymously_Processed_Information.pdf. Acesso em: 5 de out. de 2021.

CS que tece um espectro amplo ao defini-los como quaisquer dados relativos a uma pessoa física viva que[169]:

(i) identifique um determinado indivíduo pelo nome completo, NRR, imagem ou semelhante,

(ii) mesmo se, por si só, não identifique um determinado indivíduo, pode ser facilmente combinada com outras informações para identificar um determinado indivíduo, ou

(iii) são informações nos itens (i) ou (ii) acima que são pseudonimizadas e, portanto, tornam-se incapazes de identificar um determinado indivíduo sem o uso ou combinação de informações adicionais, para restauração ao estado original.

Enquanto a legislação coreana tende a enumerar detalhadamente as hipóteses regradas, a japonesa normalmente adota forma mais genérica. Na LPIP-JP apenas há a determinação de que as informações pessoais são aquelas armazenadas em um banco de dados que permite a fácil recuperação das informações nele contidas.[170]

As distinções entre os dois ordenamentos se devem, em grande parte, à forma como a história recente dos países se desenvolveu, conforme observamos nos capítulos 3 e 4. Enquanto a Coreia segue um modelo mais rígido, tendo em vista um passado recente de governo por um regime militar, o Japão mantém a estrutura naturalmente burocrática junto de um modelo jurídico com relaxamento dos direitos e responsabilidades nessa área.

Por mais que a forma como ambos os ordenamentos abarcam a proteção de dados seja semelhante em conteúdo, devido às diversas características compartilhadas, as diferenças se devem justamente ao desenrolar histórico contemporâneo de cada um dos países. Tais divergências podem ser evidenciadas ao observarmos a inserção dessas nações no cenário internacional, mais especificamente, quanto à decisão de adequação da Comissão Europeia.

5.1.2 Direitos e responsabilidades

Primeiramente, ambos os ordenamentos de proteção de dados possuem previsões muito parecidas quanto aos direitos e responsabilidades de um CDP. Contudo, a forma como

---

[169] SOUTH KOREA. **PERSONAL INFORMATION PROTECTION ACT**. 2020. Definition; Article 2. Disponível em: https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=3. Acesso em: 25 de set. de 2021.

[170] JAPAN. **Amended Act on the Protection of Personal Information**. 2020. Definition; Article 2: (6). Disponível em: https://www.ppc.go.jp/files/pdf/APPI_english.pdf. Acesso em: 10 de out. de 2021.

esses estão previstos e implementados é bem distinta. A República da Coreia, por seu turno, abarca tais medidas de segurança em na LPIP-CS;[171] já o Japão opta por determinar tais medidas por meio de diretrizes gerais.[172]

Quanto aos direitos e responsabilidades abarcados pelo ordenamento japonês, as exceções e relaxamentos em diversos aspectos do instituto de proteção de dados nipônico são diversos. Dito isso, conforme apresentado no capítulo 3, as diretrizes gerais de medida de segurança japonesas relaxam os padrões para um controlador/operador de empresa de pequeno ou médio porte.[173] Enquanto isso, na Coreia do Sul, o mais próximo que pode ser visto como uma medida de relaxamento se encontra nas Emendas de 2020, em que a necessidade de consentimento do titular de dados foi removida em alguns casos. O legislador sul-coreano diante de circunstâncias que cercam a coleta e práticas de manuseio habituais, compreendeu que não resultará em qualquer desvantagem para o titular dos dados essa prática.[174]

Uma medida na qual a Coreia do Sul se diferencia é quanto às previsões expressas da terceirização de dados por parte do CDP. Enquanto no ordenamento japonês existem recomendações para que tal procedimento seja feito, a LPIP-CS determina expressamente um modelo para que isso ocorra da forma mais segura e efetiva possível. Uma das formas estabelecidas pelo ordenamento sul-coreano, nesse caso, é a responsabilidade em pseudonomizar e anonimizar os dados.

A pseudonimização e anonimização de dados é matéria recepcionada por ambos os países, contudo, existe uma diferença sensível entre a forma como cada um dos ordenamentos desenvolve esses pontos. A LPIP-CS se limita a regrar sobre os temas como um tratamento de dados pessoais, de forma a minimizar qualquer possível violação da privacidade dos titulares, devendo anonimizar os dados e, se o anonimato não for possível, pseudonimizando os dados antes do processamento.

No caso do ordenamento japonês, tanto a pseudonimização quanto a anonimização são matérias amplamente disciplinadas tanto pela CPPI quanto pela a LPIP-JP. Um CDP que

---

[171] SOUTH KOREA. **PERSONAL INFORMATION PROTECTION ACT** Principles for Protecting Personal Information; Art. 3, (4, 6, 7 e 8)., 2020. Disponível em: https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=3. Acesso em: 25 de set. de 2021.

[172] PERSONAL INFORMATION PROTECTION INFORMATION COMMISSION. **法令・ガイドライン等**. 2021. Disponível em: https://www.ppc.go.jp/personalinfo/legal/. Acesso em: 10 de out. de 2021.

[173] JAPANESE PERSONAL INFORMATION PROTECTION COMMISSIONN SECRETARIAT. **個人情報の保護に関する法律についてのガイドライン (通則編).** 3.3 (1, 2, 3 e 4) e 8 (1, 2, 3, 4, 5 e 6), 2016. Disponível em: https://www.ppc.go.jp/files/pdf/210101_guidlines01.pdf. Acesso em: 28 de out. de 2021.

[174] SOUTH KOREA. **Act on the Protection, Use, ETC. of Location Information (Special Law).** 2020. Disponível em: https://www.privacy.go.kr/eng/laws_view.do?nttId=8189&imgNo=1. Acesso em: 1 de out de 2021.

processa informações pseudônimas/anônimas não pode divulgar os métodos de conversão das informações pessoais do titular ou qualquer processo usado, para verificar a pseudonimização. Como características individuais de cada uma das espécies, o controlador de informações processadas de forma pseudônima deve tomar medidas de segurança, para evitar o vazamento de informações processadas de forma pseudônima, assim como supervisionar e controlar uma pessoa contratada para processar tais informações. Quanto às informações anônimas, por seu turno, as mesmas devem ser tornadas públicas.[175]

Contudo, aqui, novamente, podemos constatar o relaxamento de vários aspectos por parte do ordenamento japonês; por exemplo: (i) o propósito de utilização pode ser alterado além do escopo razoavelmente relacionado ao propósito original de utilização, mesmo após a criação ou aquisição de informações processadas de forma pseudônima; (ii) as obrigações gerais de notificar o PPC e os titulares de uma violação de dados não são aplicáveis e (iii) o direito do titular de acesso, correção ou pedido de cessação de uso não são aplicáveis.[176]

A pseudonimização e anonimização de dados serve como um bom exemplo para compreendermos uma diferença fundamental apresentada em ambos os ordenamentos. A preocupação do Japão se encontra atrelada ao controlador de dados, às medidas a serem tomadas por esse e aos relaxamentos para o uso de tal ferramenta. Já a República da Coreia demonstra uma preocupação inerente específica com o titular dos dados e com a forma como devem ser tratados, visando a minimizar qualquer possível violação da privacidade dos titulares, devendo anonimizar os dados e, se o anonimato não for possível, pseudonimizando os dados antes do processamento.

Agora, quanto aos direitos e responsabilidades do processador de dados, os ordenamentos, por mais que sigam por caminhos semelhantes em aplicação, são distintos em forma. Nem a LPIP-JP, nem quaisquer regulamentos relacionados, impõem quaisquer obrigações diretas a eles. No entanto, se o controlador dos dados quiser realizar um acordo com um processador dos dados, são necessárias medidas de supervisão sobre quaisquer terceiros delegados, para lidar com os dados pessoais. De modo diverso, a LIPI-CS determina que os dados estarão sujeitos às mesmas obrigações legais aplicáveis aos manipuladores de

---

[175] JAPAN. **Amended Act on the Protection of Personal Information**. 2020. Definition; Article 2: (6). Disponível em: https://www.ppc.go.jp/files/pdf/APPI_english.pdf. Acesso em: 10 de out. de 2021. Op cit., Art. 38.

[176] JAPANESE PERSONAL INFORMATION PROTECTIONN COMISSION SECRETARIAT. **個人情報の保護に関する法律についてのガイドライン (匿名加工情報編).** 2016. Disponível em: https://www.ppc.go.jp/files/pdf/guidelines04.pdf. Acesso em: 27 de set. de 2021.

dados. No caso de violação, o processador de dados será considerado um funcionário do manipulador de dados e o manipulador de dados terá responsabilidade indireta.[177]

Um elemento que chama muito atenção é a previsão especifica da LPIP-CS com os funcionários a serem nomeados pelos manipuladores de dados. Esses últimos, conforme mencionado previamente, devem nomear uma pessoa especifica para representar a empresa, ou até mesmo um funcionário público, no caso de uma instituição pública.[178] De forma completamente oposta, as previsões legais feitas pelo governo japonês, não estabelece quaisquer tratamento diferenciado nessa matéria para grande e pequena-média empresa, ou uma previsão para as instituições públicas.

Ao compararmos os direitos do titular de dados, ambos os ordenamentos garantem o direito de exigir acesso aos mesmos, para conferi-los, modificá-los ou até mesmo excluí-los. Contudo, o Japão se diferencia por apresentar diversas situações em que os titulares perdem os direitos de acesso, revisão, correção, alteração e exclusão de dados; o que não se efetiva na Coreia do Sul. Outro elemento de destaque presente na legislação japonesa, que se diferencia do regramento sul-coreano, é a previsão de perda de direitos dos titulares, no caso de os dados pessoais serem apagados no prazo de seis meses após a coleta. O mesmo pode ocorrer no caso de o fornecimento de dados resultar em algum tipo de lesão, tanto para o próprio banco de dados quanto para algum titular.[179]

A LPIP-CS inclui regras processuais prescritivas para assegurar o exercício dos referidos direitos pelos titulares dos dados.[180] Além de previsão especifica, nos termos da LUPIC, os titulares das informações de crédito terão o direito à portabilidade de dados. Especificamente, os titulares detêm o direito de solicitar aos provedores/usuários de informações que as transmitam aos próprios sujeitos das informações de crédito ou a outros indivíduos designados pelo sujeito das informações.

Em suma, quanto aos direitos e responsabilidades, é possível consolidar ainda mais a abordagem de ambos os institutos de proteção de dados. Diante das informações apresentadas, é visível que os ordenamentos possuem previsões legais muito semelhantes; contudo, seguem por caminhos diferentes para fins de aplicação. O instituto regido pela LPIP-JP é bem mais

---

[177] KANG, Minchae. **South Korea - Data Protection Overview.** OneTrust – Data Guidance, 2021. Disponível em: https://www.dataguidance.com/notes/south-korea-data-protection-overview. Acesso em: 6 de out. de 2021.

[178] Ibid.

[179] JAPANESE PERSONAL INFORMATION PROTECTION COMMISSION SECRETARIAT. **個人情報の保護に関する法律についてのガイドライン (通則編).** 2016, 2.7 (1,2,3 e 4). Disponível em: https://www.ppc.go.jp/files/pdf/210101_guidlines01.pdf. Acesso em: 28 de set. de 2021.

[180] SOUTH KOREA. **PERSONAL INFORMATION PROTECTION ACT** Principles for Protecting Personal Information; Art. 3, (4, 6, 7 e 8)., 2020. Disponível em: https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=3. Acesso em: 25 de set. de 2021.

brando quanto às responsabilidades de quem controla os dados e quanto aos direitos dos titulares. Tal indulgência, conforme já destacado, guarda total consonância com a bagagem cultural dos costumes morais prescindirem o direito para a sociedade nipônica – fato que será mais evidenciado ao analisarmos a forma como as sanções são aplicadas em cada um dos ordenamentos.[181]

Em contrapartida, o instituo de proteção de dados sul-coreano prevê relaxamentos nos pontos analisados por este trabalho. Como referido no capítulo 4, os regimes dominados pelos militares da Coreia do Sul detinham um aparelho de vigilância estatal muito forte, o que é de extrema relevância para compreender a forma como a proteção de dados é vista no país.[182] O ordenamento sul-coreano demonstra forte senso de vigilância, através da preocupação tanto com o setor público quanto com o privado; aspecto que aponta para uma grande rigidez quanto aos direitos e responsabilidades previstos pelo instituo no país.

As características apresentadas por ambos os ordenamentos, relativas a direitos e reponsabilidades, tornam-se mais claras, quando observadas sob a luz do vazamento de dados e das respectivas sanções. Tal aspecto salienta as características já destacadas tanto no Japão quanto na Coreia do Sul.

5.1.3 Notificação de vazamento dos dados e sanções

Por fim, ao compararmos a notificação de vazamento de dados, é saliente a diferença de abordagem em ambos os ordenamentos. Como exemplo, no Japão a regulação do tema ocorre por meio de diretrizes emitidas pela CPP, enquanto que, na Coreia do Sul, essa está integralmente na LPIP-CS. Quando da ocorrência de vazamento de dados, conforme discutimos acima ao tratamos dos direitos e responsabilidades, as atitudes esperadas do controlador de dados, em ambos os ordenamentos, são bastante distintas. No Japão, podemos encontrar o termo “desejável”, o que ressalta o caráter de recomendação e não de uma responsabilidade direta, a ser tomada pelo responsável do vazamento de tais dados. O ordenamento sul-coreano, diferentemente, usa o termo “deve” ou, em outras palavras, compreende a questão da notificação de vazamento de dados como um dever, por parte de quem maneja esses dados, de prontamente informar os titulares acerca de eventual vazamento.

---

[181] DAVID, Renê. **Os Grandes Sistemas do Direito Contemporâneo**. 5ª. Ed. São Paulo: Martins Fontes – selo Martins, René David: tradução Hermínio A. Carvalho, 2014. p. 607 e 608.

[182] ROBINSON, Michael Edson. **Korea's Twentieth-Century Odyssey: A Short History**. Honolulu: University of Hawaii Press, 2007.

No Japão, a CDP sugere, por meio de diretrizes, um passo a passo no caso de vazamento. Os procedimentos entre ambos os países são similares quanto à notificação, por mais que exista uma diferença de foco na forma com que ambos são abordados. A LPIP-CS tem um grande foco no titular e na celeridade do processo de notificação de vazamento. Já as diretrizes emitidas pelo governo japonês se preocupam com a rápida notificação do vazamento para os titulares; a menos que os dados estejam criptografados em "alto nível". Contudo, as normas nipônicas demonstram diversas medidas a serem tomadas pelo próprio controlador de dados, para identificar mais informações, bem como para prevenir a ampliação/agravamento de qualquer dano, planejar e implementar medidas para prevenir a recorrência do incidente ou outros incidentes que possam ocorrer. As medidas aplicadas para garantir essa segurança são apresentadas juntamente com o relato do vazamento de dados.

Um elemento que cabe destaque, na LPIP-CS, é a celeridade no processo de vazamento. Ao tomar conhecimento de uma violação dos dados pessoais, o manipulador deve, prontamente, agir e notificar cada um dos titulares afetados em tal vazamento. Além disso, quanto às obrigações setoriais, tanto os PSICs quanto os destinatários dos dados pessoais fornecidos pelos PSICs estão sujeitos às disposições especiais sobre os PSICs. Portanto, a notificação deve ser fornecida aos titulares dos dados e à CPIP-CS ou à instituição especializada.[183]

Diferente do ordenamento japonês, a lei sul-coreana prevê uma disposição diversa para vazamentos de casos menores (menos de 1.000 titulares) e casos maiores (mais de 1.000 titulares). Em ambos, a LPIP-CS prevê a notificação imediata sobre o vazamento de dados aos titulares. Contudo, em um caso de vazamento maior, o manipulador de dados deve relatar a violação a uma instituição especializada designada pela LPIP-CS, trazendo uma previsão direta da divulgação das informações de vazamento em *homepage* da Internet ou em locais visíveis do respectivo estabelecimento comercial.[184]

Outro ponto merecedor de destaque no ordenamento japonês, diz respeito ao fato de que o controlador pode optar por qual medida tomar, em relação ao vazamento, havendo recomendação de que uma notificação geral aos titulares afetados seja efetuada, juntamente de uma direta/individual. Deve ser levada em consideração a gravidade da perda e o dano que a

---

[183] SOUTH KOREA. **PERSONAL INFORMATION PROTECTION ACT**. Safeguards of Personal Information; Article 29, 2020. Disponível em: https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=3. Acesso em: 25 de set. de 2021.

[184] SOUTH KOREA. **PERSONAL INFORMATION PROTECTION ACT.** Data Breach Notification; Article 34., 2020. Disponível em: https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=3. Acesso em: 25 de set. de 2021.

mesma pode causar. O controlador deve atendar para a eficácia dos meios de notificação. As diretrizes do governo japonês determinam que, se uma perda, eventualmente, causar danos graves, o curso de ação prudente é torná-la pública imediatamente e, posteriormente, notificar as partes afetadas de modo individual. Contudo, as diretrizes não especificam o que configura um agir imediato.

Enquanto, no Japão, as diretrizes sugerem uma recomendação para evitar possíveis problemas decorrentes do vazamento de dados, a LPIP-CS tem uma previsão clara quanto a medida cogente a ser seguida. Outro elemento diverso entre ambas as normas está na forma como a celeridade de tal notificação é prevista. Ambas apresentam a necessidade de agilidade para informar o titular do vazamento de dados. Contudo, apenas a Coreia do Sul prevê um prazo de 24 horas para a notificação.[185]

Além da celeridade, as disparidades estruturais de notificação são claras ao observarmos ambos os ordenamentos. A preocupação do legislador da LPIP-CS tem como foco principal os direitos do titular dos dados, a fim de construir o que deve ser feito a partir dessa base. Como o histórico de privacidade na Coreia do Sul é fator de relevância para a sociedade, a preocupação com a segurança dos dados do titular é o principal elemento de suporte fático da norma. Ao contrário da situação coreana, o sistema japonês parte do elemento central relacionado ao vazamento dos dados, para depois notificar o titular.

A abordagem das diretrizes japonesas inclui uma forma mais ampla de lidar com os vazamentos de dados. As medidas recomendadas são extremamente didáticas, mas por não apresentarem clareza no norte central de atuação, tornam-se demasiadamente burocráticas, diferindo do sistema mais simples previsto pela LPIP-CS.

No que tange às sanções, ambas especificam punições para o vazamento de dados. No caso do Japão, é observável a influência do "desvio" do ordenamento jurídico, como forma de norte para práticas das relações sociais presentes na cultura nipônica, no ordenamento de proteção de dados. A compensação oferecida às partes afetadas por vazamentos, tanto para prevenir quaisquer procedimentos processuais quanto para manter boas relações públicas, é uma demonstração da forma como o ordenamento é, de fato, aplicado no país. Ainda mais, salvo em casos identificados como mais graves, os custos processuais inviabilizariam qualquer tipo de medida judicial, para reparar possíveis dados. [186] Contudo, por mais que

---

[185] SOUTH KOREA. **PERSONAL INFORMATION PROTECTION ACT**. Safeguards of Personal Information; Article 29, 2020. Disponível em: https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=3. Acesso em: 25 de set. de 2021.

[186] Daniel. **Japan - Data Protection Overview**. OneTrust – Data Guidance, 2021. Disponível em: https://www.dataguidance.com/notes/japan-data-protection-overview. Acesso em: 6 de out. de 2021.

medidas judiciais sejam, muitas vezes, inviáveis, é costumeiro o ressarcimento de prejuízos decorrentes de vazamento de dados. Uma possível prática por parte de CPPs, conforme aludido no capítulo 3, é a aplicação do *giri*, segundo o qual a indenização ao titular passa a ser um dever moral, por mais que o causador do dano não esteja sendo obrigado a tal.

Em direção oposta ao precedente judicial, observamos um exemplo de grave vazamento, em que o ressarcimento não foi aplicado de forma voluntária. Trata-se do caso judicial da Benesse Holdings Inc., no qual ocorreu o vazamento de dados pessoais de 29 milhões de clientes.[187] A decisão se voltou exatamente para a aplicação de uma multa, diferentemente do que podemos observar pelo ordenamento coreano, em que a esfera de responsabilização pode ser muito maior.[188]

A norma da Coreia do Sul, distintamente da do Japão, expressamente determina todas as possíveis responsabilizações que um controlador poderá enfrentar diante de um vazamento de dados. As sanções podem ser movidas por reguladores (CPIP-CS, a CCC e a CSF), impondo diversas sanções administrativas e promotores públicos, através de punições na esfera criminal e por responsabilização civil em benefício de titulares de dados, que sofram danos como resultado de tais violações.[189]

As decisões sul-coreanas relatadas no presente estudo revelam preocupação com os cuidados específicos ao titular de dados; por exemplo, através de vários mecanismos para fazer cumprir efetivamente os direitos e obter reparação. Há os Centros de Atendimento à Privacidade, operados pela KISA, e os Comitês de Mediação de Disputas[190]. O Supremo Tribunal[191] coreano, inclusive, já decidiu no sentido de invalidar o consentimento obtido de titulares em circunstâncias que haviam dificultado a estes a compreensão clara do que haviam consentido. Em outra decisão[192], o Tribunal Superior julgou o próprio agente público (Centro de Informações Farmacêuticas da Coreia) entendendo que os dados dos titulares estavam efetivamente com os padrões de proteção adequados.

Por fim, diante das sanções aplicadas tanto na Coreia do Sul quanto no Japão, é evidenciada perceptiva diferença entre o sistema extremamente burocrático japonês e a

---

[187] THE JAPAN TIMES. **Benesse data thief gets 3½ years in prison, ¥3 million fine.** The Japan Times Ltd, 2016. Disponível em: https://www.japantimes.co.jp/news/2016/03/29/national/crime-legal/benesse-data-thief-gets-3%C2%BD-years-prison-¥3-million-fine/. Acesso em: 27 de set. de 2021.

[188] Daniel. **Japan - Data Protection Overview**. OneTrust – Data Guidance, 2021. Disponível em: https://www.dataguidance.com/notes/japan-data-protection-overview. Acesso em: 6 de out. de 2021.

[189] SOUTH KOREA GOVERNMENT. Op cit., 57.

[190] GREENLEAF, Graham. **The Draft Korea Adequacy Decision: Submission to European Union Authorities.** University of New South Wales Law Research Series, 2021. p. 11.

[191] Supremo Tribunal da Coreia do Sul. **Decissão 2016 Do13263.** 2016.

[192] Tribunal Superior de Seul. **Decisão: 2017Na2074963/2017Na2074970.** 2017.

rigidez punitiva do sistema sul-coreano. Enquanto a ocorrência de vazamento de dados, previsto nas diretrizes do governo japonês, recebe indicativo de "opção" a ser seguida, no caso da LPIP-CS, um caso de vazamento de dados é cogente e claro, ao apresentar o caminho que deve ser seguido. Enquanto a LPIP-CS especifica os inúmeros tipos de responsabilizações possíveis para o controlador de dados, a CPP, por meio de diretrizes, estabelece que a maior responsabilização japonesa se restringe a multas, em caso de vazamentos. Aqui a visão de privacidade de ambos os países estabelece os respectivos modelos de atuação punitiva. No caso do Japão, a própria repercussão social da quebra de confiança é a grande penalização, enquanto, para os sul-coreanos, as sanções pecuniárias têm o caráter de coibir a violação dos direitos de titulares de dados.

5.2 Impactos na decisão de adequação

Como destacado acima, a adequação do instituto da proteção de dados às normas da UE se encontra disciplinada sob o artigo 45º do RGPD da Comissão Europeia. A previsão legal assegura segurança aos dados tutelados no âmbito da comunidade europeia. Assim, a adequação busca, precipuamente, a efetividade e a segurança da proteção de dados tratados no âmbito da UE e compartilhados com outros países. Contudo, a aplicação e a compreensão da forma como a decisão de adequação de fato ocorre só está sendo compreendida atualmente, como sustentaremos adiante. Uma vez finalizada, a decisão de adequação da Comissão Europeia relativa à República da Coreia será a terceira decisão desse tipo no âmbito do RGPD. Para Greenleaf, a decisão é significativa não apenas pelas implicações práticas para a Coreia, mas também pelo que acrescenta ao nosso entendimento emergente de como a adequação está sendo interpretada no GDPR.[193]

Tal relevância do entendimento da decisão de adequação ocorre devido aos dois exemplos anteriores – Japão e Reino Unido – não demonstrarem um real panorama para a implementação dessa decisão. Nesse sentido, Greenleaf[194] sustenta que:

> o projeto de decisão, em relação ao setor privado, não contém justificação suficiente de que o Japão cumpre os critérios de adequação da UE, descritos em a Decisão exige que o Japão "garanta um nível de proteção 'essencialmente equivalente' ao assegurado" na UE.

[193] GREENLEAF, Graham. **The Draft Korea Adequacy Decision: Submission to European Union Authorities**. University of New South Wales Law Research Series, 2021.
[194] GREENLEAF, Graham. **Japan: EU Adequacy Discounted**. University of New South Wales Law Research Series, 2018, p. 8.

No ano de 2018, um ano antes da decisão de adequação do Japão entrar em vigor, Greenleaf elencou uma série de elementos que justificavam - e ainda sustentam – o entendimento apresentado acima.[195] Como exemplo, o autor destaca que a exigência do exercício dos direitos do titular dos dados seja eficaz e aplicável, além de que haja uma reparação judicial e administrativa efetivas. Apesar de ser evidente que a execução e a reparação devem ser demonstradas na prática, a decisão quanto à adequação do Japão ignora essa necessidade. As diferenças culturais apontadas no decorrer deste estudo podem ajudar a explicar as distinções no quantum das penalidades, mas não podem explicar a aplicação em um cenário internacional.[196] Cabe lembrar, que, como transcrito anteriormente, o Artigo 45, nº 2, "a" é explicito no direcionamento de observância da efetividade da proteção dos dados e na garantia ao exercício dos direitos sobre esses. [197]

A ampla extensão das medidas de relaxamento adotadas pelas normas japonesas, cabe, também, ser destacada. A decisão de adequação não se aplica a um leque muito amplo de categorias de operadores de negócios quando eles estiverem processando dados pessoais para fins específicos, conforme definido pela LPIP-JP.[198] Tais excludentes são vistos, por exemplo, no caso de dados pseudônimos/anônimos, no qual o propósito de utilização pode ser alterado além do escopo razoavelmente relacionado ao propósito original de utilização, mesmo após a criação ou aquisição de informações processadas de forma pseudônima.[199]

Outro ponto de relevância é a confiabilidade das traduções de documentos importantes relativos à proteção de dados. Diante de um cenário de internacionalização das normas de proteção de dados, é essencial que a tradução em que se baseia uma decisão de adequação seja tão confiável quanto possível. A tradução em inglês da LPIP-JP afirma que "não teve seus textos verificados por um falante nativo de inglês nem por um editor de língua jurídica e, portanto, pode estar sujeito a alterações", e que apenas os "textos jurídicos originais

---

[195] Vale ressaltar que os mesmos elementos também foram constatados no decorrer deste trabalho e se demonstram realçados após a comparação de ambos os países. Vale ressaltar que os mesmos elementos também foram constatados no decorrer deste trabalho e se demonstram realçados após a comparação de ambos os países.

[196] GREENLEAF, Graham. **Japan: EU Adequacy Discounted**. University of New South Wales Law Research Series, 2018, p. 8.

[197] EUROPEAN COMMISSION. **Adequacy decisions How the EU determines if a non-EU country has an adequate level of data protection.** 2021. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Acesso em: 27 de set. de 2021.

[198] GREENLEAF, op cit., p. 9.

[199] Japanese Personal Information Protection Commission Secretariat. **個人情報の保護に関する法律についてのガイドライン (匿名加工情報編).** 2016. Disponível em: https://www.ppc.go.jp/files/pdf/guidelines04.pdf. Acesso em: 27 de set. de 2021.

japoneses" estão em vigor. Isso também se aplica à versão japonesa das Regras Suplementares, que são presumivelmente oficiais.[200]

Conforme mencionado na nota de rodapé de número 75, no capítulo 3, o acesso às normas do ordenamento japonês, para a elaboração do presente estudo foi difícil, tendo sido necessário recorrer ao texto original, pois as informações disponíveis, no site oficial do governo para a proteção de dados do Japão, não contêm nem mesmo metade das informações necessárias para desenvolver o presente estudo. Considerando o caráter evidentemente internacional do universo de tratamento de dados no mundo globalizado pela *web*, esse elemento de acesso às normas – detalhamentos existentes apenas no idioma japonês – é fator que impõe barreira à efetividade da adequação. Importante frisar que, no caso da Coreia do Sul, tal problema não foi evidenciado. No site oficial do governo sul-coreano sobre a proteção de dados, todas as informações se encontram disponíveis tanto em língua inglesa quanto na coreana.[201]

A falta de obrigatoriedade nas medidas a serem tomadas por um controlador de dados, e as lacunas quanto à notificação de violação de dados também mereceram destaque.[202] As medidas que devem ser tomadas por um controlador, em sua maioria, conforme evidenciado previamente, tem apenas o caractere de recomendação, e nunca de obrigatoriedade. Enquanto a notificação de violação de dados é feita da mesma forma, apenas na forma de sugestão e nunca como uma obrigatoriedade.

Na época de emissão da decisão de adequação com o Japão, embora fosse claro que a proteção "essencialmente equivalente" não estivesse presente, o projeto de decisão não explica por que essas omissões e deficiências não devem impedir uma avaliação de adequação positiva aqui. Para a primeira decisão de adequação sob o GDPR, essa abordagem não resulta em um caso convincente para a adequação do Japão, nem fornece um guia para o que é necessário, para uma proteção equivalente ao proposto pela UE.[203]

Desse modo, na tentativa de unificação mundial de proteção de dados pela União Europeia, a forma como a proteção deve ser observada, no âmbito internacional, torna questionáveis as características regionais presentes em um ordenamento. Aqui o Japão se destaca na forma como aborda a proteção de dados; as diretrizes, por mais que tenham poder

---

[200] GREENLEAF, Graham. **Japan: EU Adequacy Discounted**. University of New South Wales Law Research Series, 2018. p. 9.

[201] EUROPEAN COMMISSION. **Adequacy decisions How the EU determines if a non-EU country has an adequate level of data protection.** 2021. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Acesso em: 27 de set. de 2021.

[202] GREENLEAF, op cit., p. 9.

[203] Ibid., p. 9.

de lei, raramente o fazem, devido à utilização como recomendação. De acordo com a cultura do país, o ordenamento japonês de modo "esperançoso" espera que uma empresa, no caso de vazamento de dados, adote as melhores medidas possíveis, para realizar a notificação e se dispor de boa vontade a pagar possíveis compensações aos dados vazados. Assim, tal noção garante um caráter extremamente vago quanto a proteção de dados no ordenamento. Por mais que essa forma de fazer direito possa ser efetiva para a nação, ainda assim, não se demonstra legítima, ao observarmos um cenário internacional, aqui, especificamente, os padrões estabelecidos pela União Europeia.

Para garantir que os padrões da UE sejam seguidos, conforme mencionado no Artigo 45, nº 3, do RGPD, e referido no capítulo 2, a decisão de adequação prevê um procedimento de avaliação periódica, de, no mínimo, a cada quatro anos. Tal procedimento deverá levar em conta todos os desenvolvimentos determinados como pertinentes pela UE, levando considerando país ou organização internacional.[204] No caso do Japão, a decisão de adequação determinou que as revisões periódicas tenham o prazo reduzido de quatro para dois anos. Tais revisões se dão, em grande medida, devido a certas exigências emitidas pela Comissão Europeia, para adequar o nível de proteção em ambos os países. Por mais que o governo japonês já preveja reformas constantes nas normas de proteção, o papel desempenhado pela UE é de extrema relevância. No caso do Japão, existe uma grande desconfiança quanto ao real nível de proteção pela União Europeia.[205]

Quanto às reformas presentes nas normas de proteção de dados sul-coreanas, as revisões fizeram parte desde o início dos diálogos com a Comissão Europeia. As negociações visavam promover a alteração do ordenamento coreano de modo a que este convergisse em direção aos padrões para a transferência de dados com a zona do euro; por exemplo, por meio das revisões quanto à pseudominização.[206]

Assim, as reformas levaram a Comissão Europeia a negociar com a Coreia dois documentos-chave adicionais à legislação coreana existente, tais documentos ligados diretamente com (i) as salvaguardas adicionais estabelecidas na Notificação n.º 2021-1 da CPIP-CS e (ii) o que diz respeito ao direito penal e às questões de segurança nacional,

---

[204] EUROPEAN COMMISSION. **Adequacy decisions How the EU determines if a non-EU country has an adequate level of data protection.** 2021. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Acesso em: 27 de set. de 2021.

[205] GREENLEAF, Graham. **Japan: EU Adequacy Discounted**. University of New South Wales Law Research Series, 2018. p. 11.

[206] GREENLEAF, Graham. **The Draft Korea Adequacy Decision: Submission to European Union Authorities.** University of New South Wales Law Research Series, 2021. p. 7

garantindo o compromisso por parte das autoridades governamentais coreanas perante a Comissão.

Primeiramente, as salvaguardas adicionais são uma notificação feita pela CPIP-CS com base nos artigos 5 (Obrigações do Estado, etc.) e 14 do LPIP-CS (Cooperação internacional). Eles fornecem esclarecimentos que se aplicam a qualquer processamento de dados pessoais no âmbito do LPIP-CS, bem como salvaguardas adicionais para dados pessoais transferidos para a Coreia, com base na decisão de adequação.

Desse modo, em relatório, a Comissão concluiu que o sistema coreano garante a aplicação efetiva das regras de proteção de dados na prática, garantindo assim um nível de proteção essencialmente equivalente ao do GDPR. Destaque-se que essa conclusão se baseia na aplicação efetiva das regras na prática e não apenas no que consta na face da legislação. Talvez a crítica mais significativa quanto à decisão do Japão seja que essa não se baseou na aplicação efetiva, principalmente, porque poucas evidências de aplicação real existem.[207]

O ordenamento coreano, conforme ressaltado neste estudo, abarca de modo amplo a aplicação dos direitos individuais. Tal aplicação ocorre por meio de reparações administrativas e judiciais eficazes, incluindo indenização por possíveis danos; elemento esse compreendido como basilar, pela Comissão Europeia para a decisão de adequação.[208]

O fornecimento de mecanismos pelo sistema coreano fornece aos indivíduos vários mecanismos para fazer cumprir efetivamente os direitos e obter reparação (judicial). Incluem-se aqui as obrigações dos controladores e a operação de instituições corretivas especializadas. Além disso, existem disposições para uma mediação de conflitos coletivos, com ações daí resultantes. Finalmente, existem disposições no LPIP-CS para ações corretivas a serem tomadas perante um tribunal que podem resultar em compensação por danos reais ou, alternativamente, danos legais de até US$ 3.000, sem necessidade de provar o dano real.[209]

A conclusão geral da Comissão Europeia é de que o sistema coreano oferece várias vias para obter a consolidação dos direitos dos titulares, destacando as opções de baixo custo e fácil obtenção; por exemplo, Call Center de Privacidade ou mediação coletiva. O que contrasta, mais uma vez, com a decisão do Japão, em que nenhuma conclusão nessa direção foi tomada.[210]

---

[207] REENLEAF, Graham. **The Draft Korea Adequacy Decision: Submission to European Union Authorities.** University of New South Wales Law Research Series, 2021. p. 10.
[208] Ibid., p. 11.
[209] Ibid., p. 11.
[210] Ibid., p. 11.

Desse modo, a Coreia detém a lei de privacidade de dados mais forte da Ásia na última década, junto com a aplicação mais eficaz. Uma vez que as reformas legislativas de 2020 corrigiram o descompasso entre os requisitos da UE para um acordo de processamento de dados independente e a distribuição dos poderes de execução na Coreia, o país estava bem posicionado, para ser objeto de uma decisão de adequação positiva. O aceite da Comissão sobre o sistema de proteção de dados da Coreia é um argumento forte a favor da proteção adequada.[211]

O comparativo entre os ordenamentos de proteção de dados dos dois países evidencia a existência de divergências estruturais consideráveis entre ambos, conforme apontado na primeira parte desse capítulo. Exsurge ainda do comparativo que o impacto da adoção da decisão de adequação em ambos os países é bastante diferente de um para o outro. A provável decisão de adequação da Coreia é muito mais efetiva, à luz do regramento da UE, do que a decisão da Comissão sobre o Japão. Tudo indica que a justificativa econômica decorrente do tratado comercial entre o Japão e a UE é a razão mais provável para a forma como a decisão de adequação foi estabelecida. Em uma análise rigorosa dos regramentos nas normas da UE, a legislação japonesa careceria de ajustes.

Por fim, cabe lembrar que a credibilidade da objetividade do processo de adequação é importante para a UE a longo prazo e, por esse motivo, a decisão da Coreia é um referencial muito mais relevante para uma decisão de adequação. Levando isto em conta, pode-se dizer que o avanço dos mecanismos de decisão de adequação em adoção no procedimento da Coreia busca o efetivo alinhamento das normas deste país com as adotadas na UE. O modelo sul-coreano certamente será um parâmetro para outros países que passem por este processo.

[211] REENLEAF, Graham. **The Draft Korea Adequacy Decision: Submission to European Union Authorities.** University of New South Wales Law Research Series, 2021. p. 14.

6 CONSIDERAÇÕES FINAIS

Retomando a sequência de exposição dos dados, após a introdução do tema e apresentação dos objetivos e problema de pesquisa, o 2º capítulo discorreu sobre a proteção de dados, apresentando a relevância do instituto, o histórico das origens e a decisão de adequação pela Comissão Europeia. Na primeira parte, quanto à relevância dos dados na contemporaneidade, buscou-se demonstrar como esses são um dos maiores combustíveis econômicos de nossa época; por exemplo, através das economias de plataforma. Isso posto, a segunda parte contextualizou a história da proteção de dados e da evolução das normas desse instituto. Por fim, a terceira parte do capítulo discorreu sobre a decisão de adequação pela Comissão Europeia, que é a entidade representante do bloco europeu, indiscutível precursor da proteção legal da manipulação/tratamento de dados no mundo. Em sequência, o 3º capítulo se debruçou sobre a proteção de dados no contexto do Japão, enquanto o 4º capítulo descreveu tal ordenamento no âmbito da Coreia do Sul. A análise das normas nacionais de privacidade de dados, em ambos os capítulos, detalhou: (I) o contexto histórico e político da privacidade de dados; (II) o contexto de vigilância; (III) o sistema legal; (IV) as normas de privacidade de dados e (V) a jurisprudência relacionada ao tema. No 5º capítulo, buscou-se traçar um comparativo acerca das normas de privacidade de dados entre a Coreia do Sul e o Japão. Foi tecida análise comparativa entre as normas das duas nações e os efeitos dos procedimentos de decisão de adequação às normas da UE nas mesmas.

Com base na sequência descrita, foi possível observar que os ordenamentos jurídicos, tanto do Japão quanto da Coreia do Sul, foram construídos sobre os mesmos fundamentos teóricos, praticamente todos originalmente gestados a partir da evolução normativa desenvolvida pela União Europeia. Apesar dessa base comum, a estrutura normativa de cada um dos dois países foi construída sob forte influência das culturas locais; o que confere características distintas para os ordenamentos de ambas as nações. Desta forma, levando em consideração os fatos, normas e argumentos expostos na presente análise, pode-se inferir que o ordenamento legal da proteção de dados dos dois países dispõe de forma bastante distinta quanto à previsão, aplicação e implementação da decisão de adequação, apesar de serem fundados sobre uma mesma base conceitual originada na União Europeia. Isso porque, com base nas comparações, constaram-se diferenças consideráveis entre os normativos de cada uma das nações. Posteriormente, observando os possíveis impactos de tais diferenças diante da decisão de adequação da União Europeia, verificou-se que, embora o Japão tenha obtido a decisão de adequação da Comissão Europeia, o país não se adequa a diversas exigências da

legislação da UE, o que possivelmente se deve a um acordo comercial que foi concluído juntamente com a decisão de adequação entre o bloco europeu e o Japão. Em contrapartida, a Coreia do Sul se adequa às medidas propostas pela União Europeia, e o caso do país pode servir de parâmetro para decisões de adequação futuras.

Mesmo que o nível da adequação de privacidade de dados do Japão possa ser questionável, não há dúvidas quanto à influência dos interesses econômicos entre a nação nipônica e o bloco europeu. A decisão de adequação com o Japão ocorreu juntamente com a finalização de um tratado econômico, o que justifica as inúmeras concessões feitas para a adequação japonesa. O tratado comercial motivando tal decisão representa uma evidência do que foi apresentado no 2º capítulo desta análise, em que o valor econômico relativo aos dados e a vantagem de um acordo comercial entre o União Europeia e a terceira maior economia do mundo, o Japão, foram salientados.

Em suma, evidencia-se que os ordenamentos possuem previsões legais muito semelhantes; contudo, seguem por caminhos diferentes quanto à aplicação. O instituto japonês regido pela LPIP-JP é bem mais brando quanto às responsabilidades de quem controla os dados e quanto aos direitos dos titulares. Tal identidade, conforme acima referido, guarda total consonância com a bagagem cultural e os costumes morais nipônicos, que, em muitas das respectivas relações, buscam "prescindir" do direito como fator norteador dos atos.

Por outro lado, e também por elemento da cultura, o instituto de proteção de dados sul-coreano detém vieses rígidos no ordenamento para proteger os dados dos cidadãos. Conforme destacado, como nos períodos dominados pelos militares da Coreia do Sul foram mantidos aparelhos de vigilância estatal muito fortes sobre a população, a estrutura das normas de proteção de dados (proteção da privacidade) é completa e rigorosa, na defesa da forma com que o tratamento de dados é efetivado. Desse modo, o ordenamento sul-coreano demonstra o forte senso de vigilância dos atores manipuladores de dados, o que é evidenciado através da preocupação do país tanto com o setor público quanto com o privado. Assim, esse último apresenta uma grande rigidez quanto aos direitos e responsabilidades previstos pelo instituto no país.

Por fim, diante dos fatores expostos, no que se refere à decisão de adequação, a possível decisão da Coreia é muito mais convincente do que a decisão da Comissão da UE sobre o Japão. A justificativa econômica inerente ao tratado comercial entre o Japão e a UE aparenta ser a razão mais provável para a forma como a decisão de adequação foi feita com relação a esse país. Contudo, sob a ótica de credibilidade dos objetivos do processo de adequação, é importante para a UE que esses sejam tecnicamente rígidos. No longo prazo, a

decisão da Coreia dá indícios de que poderá vir a ser um exemplo mais adequado do que o japonês. Com isso, o modelo sul-coreano pode vir a ser parâmetro para os outros países que vierem a passar por um procedimento de decisão de adequação.

Também é importante destacar que, no caso da decisão de adequação da Coreia do Sul, a adequação complementaria o Acordo de Comércio Livre entre UE-República da Coreia, o que detém o potencial de aumentar a cooperação entre a União Europeia e a Coreia do Sul, enquanto potências digitais. Contudo, nesse caso, poucas concessões foram feitas à República da Coreia para a adoção da decisão de adequação. Assim, de modo a seguir o padrão estabelecido pela Art. 45º do RGPD e da Comissão Europeia, a Coreia do Sul realizou alterações abrangentes nas leis de privacidade de dados nacionais; o que garante mais segurança jurídica para a decisão de adequação do que para a decisão do Japão.

Do todo aqui exposto, é possível concluir que o ordenamento japonês apresenta muito menos aderência aos fundamentos nascidos na UE do que o da Coreia do Sul. As adequações promovidas nas normas da Coreia demonstram-se mais aderentes aos parâmetros internacionais apresentados pela UE. Os modelos adotados pelas normas de proteção de dados, por mais que baseados em conceitos ocidentais, estão também muito calcados em uma visão cultural oriental. Tal aspecto pode gerar dificuldades quanto à proteção de dados entre União Europeia e Japão. Em contrapartida, no caso da Coreia do Sul, há indícios de convergência da cultura local às normas originadas na UE, o que garante uma maior segurança diante da proteção de dados entre o bloco e esse país. Neste momento, resta observar como os impactos da decisão de adequação com a Coreia do Sul gerarão efeitos para futuras decisões de adequação e assim para o cenário internacional de proteção de dados.

Mesmo que até o presente momento o instituto da proteção de dados esteja sendo norteado por conceitos e processos surgidos na comunidade europeia, o processo de internacionalização futuro do instituto tende a gradualmente sofrer maior influência de outras regiões do planeta. Não se deve olvidar, todavia, que eventual movimento normativo dos Estados Unidos da América, especialmente considerando a relevância econômica global desse último país, possa trazer novos direcionamentos para o âmbito da proteção de dados. Tal condição, muito provavelmente, ocorreria no conhecido contexto de oposição de interesses econômicos dos EUA em relação à comunidade europeia. Pois, muito do atual regramento emanado pela UE, foi estruturado com o intuito de regrar o uso de dados promovido por corporações estadunidenses. Esse universo de peso e contrapeso no uso de dados com interesses econômicos está apenas no inicio da respectiva formatação por sua vez.

Por fim, conscientes de não termos esgotado a matéria, esperamos ter contribuído no estudo do instituto da proteção de dados e para encorajar novas investigações sobre o tema. A proteção e a regulação desse instituto afinal é ponto de atenção da sociedade contemporânea, em que a noção de aldeia global se materializou através da integração ocorrida via internet e representa um fator indispensável para o equilíbrio entre o interesse econômico e a proteção da privacidade do indivíduo.

REFERÊNCIAS

ADAMS, Andrew; MURATA, Kiyoshi; ORIOTO, Yohko. **The Japanese Sense of Information Privacy**. AI & Society, 24 (4), 2009.

CHIBA, Masaji. **Asian legal systems: law, society and pluralism in East Asia.** Ch. 3 in Tan (Ed.), 1997.

COUNCIL OF EUROPE. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (European Treaty Series No. 108.)** 1981. Disponível em: https://rm.coe.int/1680078b37. Aceso em: 4 de set. de 2021.

DATA COMMONS. **Data Catalog WorldBank: South Korea.** 2021. Disponível em: https://datacommons.org/place/country/KOR?utm_medium=explore&mprop=count&popt=Person&cpv=isInternetUser%2CTrue&hl=en. Acesso em: 1 de set. de 2021.

DAVID, Renê. **Os Grandes Sistemas do Direito Contemporâneo**. Tradução por Hermínio A. Carvalho. São Paulo: Martins Fontes – selo Martins, 5ª. Ed, 2014.

EUROPEAN COMMISSION. **Adequacy decisions How the EU determines if a non-EU country has an adequate level of data protection.** 2021. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Acesso em: 27 de set. de 2021.

EUROPEAN COMMISSION. **Data protection: European Commission launches the process towards adoption of the adequacy decision for the Republic of Korea.** 2021. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964. Acesso em: 27 de set. 2021

EUROPEAN COMMISSION. **European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows.** 2019. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421. Acesso em: 10 de nov. de 2021.

EUROPEAN PARLIAMENT. **Resolution on the Protection of the Rights of the Individual in the Face of Developing Technical Profess in the Field of Automatic Data Processing**. 1982. Disponível em: https://op.europa.eu/en/publication-detail/-/publication/37a4ff25-4e1a-494f-bf8d-db860627910a/language-en. Acesso em: 1 de out. de 2021.

FRADERA, Véra Maria Jacob de. **A Boa Fé Objetiva, uma noção presente no conceito alemão, brasileiro e japonês de contrato.** Porto Alegre: Revista Cadernos do Programa de Pós-Graduação em Direito PPGDir./UFRGS**,** 2003.

GREENLEAF, Graham; PARK, Whon-il Park. **Korea's New Act: Asia's Toughest Data Privacy Law.** 117 Privacy Laws & Business International Report, 2012.

GREENLEAF, Graham. **Asian Data Privacy Laws: Trade & Human Rights Perspectives.** Oxford: Oxford University Press, 2014. E-book/Kindle Edition.

GREENLEAF, Graham. **Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories.** Sydney: 23(1) Journal of Law, Information & Science, University of New South Wales (UNSW Sydney), 2013.

GREENLEAF, Graham. **The Draft Korea Adequacy Decision: Submission to European Union Authorities.** Sydney: University of New South Wales Law Research Series, 2021.

HIROSHI, Kajiyama. **Digital technology can help the world prosper. Here's how.** World Economic Forum, 2021. Disponível em: https://www.weforum.org/agenda/2021/04/digital-technology-can-help-the-world-prosper-gtgs/. Acesso em: 1 de set. de 2021.HOUNSLOW, Daniel. **Japan - Data Protection Overview.** OneTrust – Data Guidance, 2021. Disponível em: https://www.dataguidance.com/notes/japan-data-protection-overview. Acesso em: 6 de out. de 2021.

INFORMATION COMMISSIONER'S OFFICE (ICO). **Adequacy.** 2021. Disponível em: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/adequacy/. Acesso em:1 de nov. de 2021.

INFORMATION COMMISSIONER'S OFFICE (ICO). **The Information Commissioner's response to the International Trade Committee Inquiry into Digital Trade and Data.** 2021. Disponível em: https://ico.org.uk/media/about-the-ico/consultation-responses/2619342/itc-digital-trade-data-response-202002.pdf. Acesso em: 26 de set. de 2021.

JAPAN. **Act. No. 151 of 1 December 2004**. Act on Promotion of Use of Alternative Dispute Resolution. 2004. Disponível em: https://www.cas.go.jp/jp/seisaku/hourei/data/AOP.pdf. Acesso em 15 de set. de 2021.

JAPAN. **Amended Act on the Protection of Personal Information**. 2016. Disponível em: https://www.ppc.go.jp/files/pdf/APPI_english.pdf. Acesso em: 10 de out. de 2021.

JAPAN. **Report by the Personal Information Protection Commission Secretariat: Anonymously Processed Information.** 2017. Disponível em: https://www.ppc.go.jp/files/pdf/The_PPC_Secretariat_Report_on_Anonymously_Processed_Information.pdf. Acesso em: 10 de out. de 2021.

JAPAN. **Report by the Personal Information Protection Commission Secretariat: Anonymously Processed Information.** 2017. Disponível em:

https://www.ppc.go.jp/files/pdf/The_PPC_Secretariat_Report_on_Anonymously_Processed_Information.pdf. Acesso em: 10 de out. de 2021.

JAPANESE PERSONAL INFORMATION PROTECTION COMMISSION SECRETARIAT. **個人データの漏えい等の事案が発生した場合等の対応について**. 2017. Disponível em: https://www.ppc.go.jp/files/pdf/iinkaikokuzi01.pdf. Acesso em: 29 de out. de 2021.

JAPANESE PERSONAL INFORMATION PROTECTION COMMISSION SECRETARIAT. **個人情報の保護に関する法律についてのガイドライン (匿名加工情報編).** 2016. Disponível em: https://www.ppc.go.jp/files/pdf/guidelines04.pdf. Acesso em: 27 de out. de 2021.

JAPANESE PERSONAL INFORMATION PROTECTION COMMISSIONN SECRETARIAT. **個人情報の保護に関する法律についてのガイドライン (通則編).** 2016. Disponível em: https://www.ppc.go.jp/files/pdf/210101_guidlines01.pdf. Acesso em: 28 de out. de 2021.

JAPANESE PERSONAL INFORMATION PROTECTION COMMISSIONN SECRETARIAT. **個人情報の保護に関する法律についてのガイドライン (通則編).** 2016. Disponível em: https://www.ppc.go.jp/files/pdf/210101_guidlines01.pdf. Acesso em 28 de out. de 2021.

KANG, H Chris; KIM, Hee Sun. **Recent major amendments to three South Korean data privacy laws and their implications.** International Bar Association, 2020. Disponível em https://www.ibanet.org/article/0D5FD702-179C-42A1-B37D-45D12F4556DA. Acesso em: 1 de out. de 2021.

KANG, Minchae. **South Korea - Data Protection Overview.** OneTrust – Data Guidance, 2021. Disponível em: https://www.dataguidance.com/notes/south-korea-data-protection-overview. Acesso em: 6 de out. de 2021.

KUNER, Christopher. **European Data Protection Law: Corporate Compliance and Regulation.** Oxford: Oxford University Press, 2nd Edition, 2007.

KWON, Youngjoon. **Korea: Bridging the Gap between Korean Substance and Western Form.** Cambridge: Cambridge University Press, Law and Legal Institutions in Asia, E. Ann Black E Gary F. Bell, Eds., 2011.

LAWSON, Carol. **Japan's New Privacy Act in Context.** Sydney: The University of New South Wales Law Journey (UNSW Law Journey), Volume 29(2), 2006.

LYNSKEY, Orla. **The Foundations of EU Data Protection Law.** Oxford: Oxford University Press, 2015.

The THE JAPAN TIMES. **Benesse data thief gets 3½ years in prison, ¥3 million fine.**, 2016. Disponível em: https://www.japantimes.co.jp/news/2016/03/29/national/crime-legal/benesse-data-thief-gets-3%C2%BD-years-prison-¥3-million-fine/. Acesso em: 27 de set. de 2021.

MIYASHI, Hiroshi. **The Evolving Concept of Data Privacy in Japanese Law**. Oxford: Oxford University Press, International Data Privacy Law, Volume 1, Issue 4, 2011.

NAÇÕES UNIDAS. **Pacto Internacional de Direitos Civis e Políticos**. (Decreto nº 592) Brasília, DF: Presidência da República, 1992. Disponível em: http://legislacao.planalto.gov.br/legisla/legislacao.nsf/Viw_Identificacao/DEC%20592-1992?OpenDocument. Acesso em: 4 de out. de 2021.

NISHITANI, Yuko. **Introdução à História do Direito Japonês.** Tradução do alemão, de Maitê Schmidtz, Luciana Quinto e revisão da Profa. Dra. Cláudia Lima Marques. Porto Alegre: Revista da Faculdade de Direito da Universidade Federal do Rio Grande do Sul, 2002.

NUNN, Adam. **The New Japanese Privacy Law: What Businesses Need to Know.** 2020. Disponível em: https://auth0.com/blog/the-new-japanese-privacy-law-what-businesses-need-to-know/. Acesso em: 25 de out. de 2021.

ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD). **Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.** 1980. Disponível em: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Acesso em: 02 de out. de 2021.

ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD). **Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.** 1980. Disponível em: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Acesso em: 02 de out. de 2021.

PARK, Whon-il. **7. Republic of Korea.** 2008. Disponível em: http://onepark.khu.ac.kr/Ch7_SKorea.pdf. Acesso em: 25 de set. de 2021.

PERSONAL INFORMATION PROTECTION INFORMATION COMMISSION. **法令・ガイドライン等**. 2021. Disponível em: https://www.ppc.go.jp/personalinfo/legal/. Acesso em: 10 de out. de 2021.

PONAZECKI, Jay; LEVISON, Daniel; MORRISON So Toshihiro. **Japan: Personal information privacy update**. Washington: BNA International World Data Protection Report, 2007. Acesso em: https://media2.mofo.com/documents/wdpr1207_privacy.pdf. Disponível em: 15 de nov. 2021.

ROBINSON, Michael Edson. **Korea's Twentieth-Century Odyssey: A Short History.** Honolulu: University of Hawaii Press, 2007.

SCHWAB, Klaus. A Quarta Revolução Industrial. Tradução de Daniel Moreira Miranda. São Paulo: Edipro, 2016.

SERRANÍA, Vanessa Jiméz; ABRUSIO, Juliana. **Big Data: Uma Análise Sob A Óptica Das Práticas Abusivas No Acesso E Uso De Dados Massificados Na Economia De Plataforma.** Florianópolis: Revista de Direito Brasileira, Florianópolis (RDBF), v. 28, Nº. 11, 2021.

SOUTH KOREA. **Act on the Protection, Use, ETC. of Location Information (Special Law).** 2020. Disponível em: https://www.privacy.go.kr/eng/laws_view.do?nttId=8189&imgNo=1. Acesso em: 1 de out. de 2021.

SOUTH KOREA. **Personal Data and Protection Law in South Korea: Laws & Policies.** 2021. Disponível em: https://www.privacy.go.kr/eng/laws_policies_list.do. Acesso em 27 de set. de 2021.

SOUTH KOREA. **PERSONAL INFORMATION PROTECTION ACT**. 2020. Disponível em: https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=3. Acesso em 25 de set. de 2021.

SOUTH KOREA. **Use and Protection of Credit Information Act.** 2018. Disponível em: https://www.law.go.kr/LSW/eng/engLsSc.do?menuId=2&section=lawNm&query=Credit%20Information&x=13&y=26#liBgcolor29. Acesso em: 1 de out. de 2021.

SUPREMO TRIBUNAL DA COREIA DO SUL. **Decissão 2016 Do13263.** 2016.

TAKAMA, Gohsuke. **Lies and Secrets - Japan's National ID Network.** Anti National ID Japan, 2002. Disponível em: https://nationalid.hantai.jp/2002/08/lies_and_secret.html. Acesso em 5 de out. de 2021.

THE ECONOMIST. **Japan Inc's IT needs a security patch.** 2020. Disponível em: https://www.economist.com/business/2020/07/18/japan-incs-it-needs-a-security-patch. Acesso em: 6 de set. de 2021.

THE JAPAN TIMES. **Uniqlo, GU brand's Fast Retailing says 460,000 online accounts were accessed in Japan hack.** 2019. Disponível em:

https://www.japantimes.co.jp/news/2019/05/14/business/corporate-business/uniqlo-gu-brands-fast-retailing-says-460000-online-accounts-accessed-japan-hack/. Acesso em: 27 de set. de 2021.

TRIBUNAL SUPERIOR DE SEUL. **Decisão: 2017Na2074963/2017Na2074970.** 2017.

TRINDADE, Manoel Gustavo Neubarth. **Economia de Plataforma (Ou Tendência à Bursatilização dos Mercados): Ponderações Conceituais Distintivas em Relação à Economia Compartilhada e à Economia Colaborativa e uma Abordagem de Análise Econômica do Direito dos Ganhos de Eficiência Econômica por Meio da Redução Severa dos Custos de Transação.** Lisboa: Revista Jurídica Luso-Brasileira (RJLB), Lisboa, Ano 6, N.º 4, 2020.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679, de 27 de abril de 2016.** Institui na União Europeia o Regulamento Geral sobre a Proteção de Dados**.** UE: Parlamento Europeu e o Conselho da União Europeia, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Acesso em: 10 de out. de 2021.

WIPO. **Global Innovation Index 2021: Tracking Innovation throught the COVID-19 Crisis.** Geneva: World Intellectual Property Organization, 2021. Acesso em: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2021.pdf. Disponível em: 10 de nov. de 2021.

MIRANDA, Pontes de. **Comentários à Constituição de 1946.** Rio de Janeiro: Editor Borsoi, 3.ª Edição, Tomo I (Arts 1.º - 5º), 1960.

EUROPEAN COMMISSION. **Data protection: Commission adopts adequacy decisions for the UK.** 2021. Disponível em: https://ec.europa.eu/commission/presscorner/detail/ro/ip_21_3183. Acesso em: 27 de set. de 2021.