A proteção dos dados pessoais em Timor-Leste

Sofia Riço Calado[1]

Resumo: Timor-Leste ainda não aprovou uma lei geral de proteção dos dados pessoais. Existem, contudo, diversas disposições legais sobre este tópico, a começar pelo artigo 38.º da Constituição. A aprovação futura de tal diploma deverá ter em conta as normas existentes, bem como poderá beneficiar da análise de soluções legislativas em vigor noutras regiões e países, em especial o Regulamento Geral sobre a Proteção de Dados da União Europeia e a Lei de Proteção dos Dados Pessoais Indonésia.

Palavras-chave: (1) dados pessoais, (2) consentimento, (3) direitos dos titulares dos dados, (4) transferências de dados, (5) Timor-Leste.

Introdução

Timor-Leste não dispõe atualmente de uma lei de proteção dos dados pessoais ou de uma autoridade de controlo. Ainda assim, faz todo o sentido escrever este artigo. Em primeiro lugar, porque a legislação timorense apresenta diversas disposições que se referem a este tópico. Aliás, a própria Constituição consagra a proteção dos dados pessoais no seu artigo 38.º.

[1] A autora é natural de Lisboa, Portugal. Atualmente, exerce funções como Senior Privacy Counsel da empresa americana Cloudflare. Entre 2020 e 2022, foi Head of Legal da subsidiária portuguesa da empresa chinesa Huawei. É licenciada e mestre em Direito pela Faculdade de Direito da Universidade Nova de Lisboa, detendo uma Pós-Graduação em Direito da Propriedade Intelectual pela Faculdade de Direito da Universidade de Lisboa. Exerceu atividade profissional em Timor-Leste entre 2006 e 2016.

Igualmente, porque a redação de normas futuras só pode beneficiar com uma análise do ordenamento já existente.

Por conseguinte, é meu objetivo mostrar-vos como o legislador tem endereçado pontualmente os aspetos relativos à própria definição de dados pessoais, às condições de licitude do tratamento, aos direitos dos titulares dos dados, aos períodos de conservação aplicáveis, entre outros.

Por outro lado, a comparação com outros enquadramentos jurídicos constitui sempre uma reflexão útil sobre a bondade e a adequação das soluções avançadas por outros países e, neste caso, sobre a sua possível relevância para Timor-Leste. Pelo que estabelecerei breves linhas de interseção com o Regulamento Geral sobre a Proteção de Dados da União Europeia (o "RGPD")[2] e a respetiva lei de execução Portuguesa[3]; bem como com a nova Lei de Proteção dos Dados Pessoais Indonésia (a "Lei Indonésia")[4].

O dispositivo constitucional

De acordo com o artigo 38.º, n.º 1 da Constituição da República Democrática de Timor-Leste (a "Constituição"), qualquer cidadão dispõe dos seguintes direitos face aos seus dados pessoais informatizados ou inseridos em registos

[2] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE, OJ L 119 de 4.5.2016, p. 1-88.

[3] Lei n.º 58/2019, de 8 de agosto, Diário da República n.º 151/2019, I.ª Série. Portugal.

[4] Lei n.º 27 de 2022, aprovada a 20 de setembro e promulgada a 17 de outubro.

mecanográficos ou pessoais: o direito de acesso, o direito de retificação ou atualização e o direito a ser informado sobre a finalidade a que se destinam.

Daqui resultam algumas pistas interessantes. Em primeiro lugar, os direitos atribuídos incidem não apenas sobre registos em suporte digital mas também sobre registos em suporte físico, quer criados por meio de máquinas como puramente escritos à mão. Este escopo de aplicação é mais alargado do que o escopo do RGPD, por exemplo, o qual exclui dados pessoais tratados manualmente que não estejam contidos ou sejam destinados a um sistema de ficheiros (ver artigo 2.º em conjunção com o recital 15).

Já os respetivos direitos decompõem-se na faculdade de ter acesso aos dados que lhe digam respeito (ainda que não tenham sido gerados pelo titular), de retificar dados inexatos ou atualizar dados que se tenham tornado obsoletos. Finalmente, deverá ser transparente para o cidadão qual o fim que preside à recolha e demais operações de tratamento dos seus dados pessoais. É para pagamento de salário, para administração de cuidados de saúde, para envio de campanhas promocionais? Seja qual for a finalidade, o titular tem o direito de saber.

Uma futura lei de proteção dos dados pessoais, segundo o artigo 38.º, n.º 2 deverá conter a definição de dados pessoais, isto é, quais são as informações classificadas como respeitantes ao indivíduo, logo merecedoras de proteção. Tanto o RGPD (ver artigo 4.º) como a Lei Indonésia (ver artigo 4.º) aplicam-se às informações que identifiquem um indivíduo ou o tornem identificável. Seria interessante definir na futura lei a disciplina aplicável aos dados pseudonimizados, ou seja, os dados

pessoais que não possam ser atribuídos a um titular de dados específico sem recorrer a informações suplementares. O RGPD considera-os dados pessoais quando a reidentificação seja possível (ver recital 26), a Lei Indonésia não faz nenhuma menção.

De igual modo, a futura lei terá que especificar as condições aplicáveis ao tratamento dos dados pessoais. Os dados pessoais apenas poderão ser tratados mediante consentimento do titular? Ou também no âmbito da celebração e execução de um contrato, para efeitos de cumprimento de uma obrigação jurídica ou da prossecução do interesse público? O interesse legítimo do responsável pelo tratamento, isto é, de quem define as finalidades e meios de tratamento, será uma condição admissível? Para o RGPD (ver artigo 6.º, n.º 1, alínea f)) e para a Lei indonésia (ver artigo 20.º, n.º 2, alínea f)) sim, mas por exemplo a legislação Chinesa não o admite[5].

Uma coisa é certa: o tratamento informatizado, i.e. em suporte digital, de dados pessoais relativos à vida privada, convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa e à origem étnica apenas poderá ocorrer com consentimento do titular, sem quaisquer exceções (ver artigo 38.º, n.º 3 da Constituição).

Antes de mais, para efeitos de definição de "dados sensíveis", quais serão os dados pessoais que constam da "vida privada" de um cidadão? Falaremos aqui de dados relativos à

[5] A este respeito, Xu Ke et al. (24 agosto 2021), "Analyzing China's PIPL and how it compares to the EU's GDPR", in The Privacy Advisor, [consultado em 14 de outubro de 2022] disponível em https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/.

saúde, vida sexual ou orientação sexual de um indivíduo, bem como de dados genéticos ou biométricos?[6]

Tal como Menezes Cordeiro refere, "o contexto (assumirá) um peso decisivo na recondução ou não recondução a esse universo" (Cordeiro, 2022: 134). Ora, os dados sensíveis são considerados como sensíveis sempre que a sua utilização possa dar origem a "tratamentos desiguais ou discriminatórios" (Miranda e Medeiros, 2017: 577). Pelo que se compreende um agravamento dos requisitos legais para o seu tratamento. Daí a imposição do consentimento pelo titular.

Todavia, mesmo o RGPD prevê mais condições de tratamento das categorias especiais de dados pessoais, por exemplo, em contexto de declaração, de exercício ou de defesa de um direito num processo judicial, ou sempre que os tribunais atuem no exercício da sua função jurisdicional (ver artigo 9.º, n.º 2, alínea f)); ou por motivos de interesse público no domínio da saúde pública (alínea i)), imaginemos numa pandemia.

Fazer depender apenas do consentimento o tratamento dos dados sensíveis vai trazer algumas dificuldades. E isto quando não é sequer 100% certo que o consentimento seja a melhor forma de garantir o controlo pelo titular. Por exemplo, é difícil para o titular avaliar, a cada situação, o que é mais ou menos vantajoso para si ou quais são as consequências associadas ao tratamento dos seus dados[7].

---

[6] O Decreto-Lei com as Regras Relativas ao Acesso a Documentos Oficiais dispõe que a recolha de dados pessoais e da vida privada, incluindo dados de saúde (sublinhado nosso), deve ser expressamente autorizado pelas pessoas a que reportam (ver artigo 16.º, n.º 1 do Decreto-Lei n.º 43/2016 de 14 de outubro, Jornal da República n.º 40 A - I.ª Série, Timor-Leste).

[7] Ver Solove, Daniel J. (2013). "Introduction: Privacy Self-Management and the Consent Dilemma". *Harvard Law Review*. Volume 126: 1880-1903.

A definição de dados pessoais

Não existindo na legislação de Timor-Leste uma definição geral de dados pessoais, até pela ausência de uma lei subordinada a este tema, é possível detetar ainda assim categorias diferentes de dados que são classificados como "dados pessoais" no âmbito dos atos legislativos que integram.

Por exemplo, o Regime Jurídico da Identificação Civil[8] elenca os seguintes dados identificadores do cidadão, de modo a estabelecer a sua identidade civil: a) número e ano do assento de nascimento e conservatória onde foi lavrado; b) se casado, nome do cônjuge; c) perda da nacionalidade; d) data do óbito (ver artigo 24.º). Aliás, os elementos identificadores do bilhete de identidade, a começar pelo próprio número e incluindo a impressão digital (considerado um dado biométrico), são seguramente dados pessoais (ver artigos 6.º a 16.º)[9].

Por outro lado, o Regime Jurídico do Recenseamento Geral da População e da Habitação[10] define que os dados estatísticos das pessoas singulares, alvo de segredo estatístico, são dados pessoais nos termos do artigo 38.º da Constituição (ver artigo 11.º, n.º 1).

[8] Decreto-Lei n.º 2/2004 de 4 de fevereiro, Jornal da República n.º 3 - I Série, Timor-Leste.

[9] O mesmo raciocínio aplica-se aos dados biográficos, imagem facial, as impressões digitais e a informação descritiva da emissão do passaporte - ver artigo 4.º do Decreto-Lei n.º 52/2016 de 28 de dezembro, Jornal da República n.º 50 - I Série, Timor-Leste.

[10] Lei n.º 1/2015 de 8 de julho, Jornal da República n.º 25 - I.ª Série, Timor-Leste.

Ainda a Lei do Recenseamento Eleitoral[11] dispõe que a base de dados de recenseamento eleitoral é composta pelos seguintes dados identificativos dos eleitores: a) número de inscrição no recenseamento eleitoral, b) unidade geográfica de recenseamento, c) nome completo, d) nome do pai e da mãe, e) data de nascimento, f) naturalidade, g) residência habitual (inclusive se no estrangeiro), assinatura e impressão digital do eleitor (ver artigo 13.º, n.º 1).

O Código de Registo Predial[12] designa que os seguintes dados considerados pessoais serão recolhidos para tratamento automatizado: a) nome e número de identificação fiscal; b) estado civil, com menção de maioridade ou menoridade quando solteiros; c) nome do cônjuge e regime de bens; d) residência habitual ou domicílio profissional (ver artigo 124.º, n.º 1).

Já a Resolução sobre o Estabelecimento do Sistema de Informação de Registo de Crédito[13] descreve como dados de crédito do mutuário os seguintes: a) nome completo, b) data de nascimento, c) documento de identificação, d) domicílio e endereço postal, e) número de telefone, f) estado civil, g) nome do cônjuge, h) histórico laboral, i) data de desembolso do crédito, j) montante total de crédito desembolsado, k) prestação mensal, l) montante atual de dívida pendente, m) classificação do crédito, n) data do último pagamento, o) tipo de colateral e, p) tipo de crédito (ver artigo 6.º). Não sendo claro quais são os dados

[11] Lei n.º 6/2016 de 25 de maio, Jornal da República n.º 20 - I.ª Série, Timor-Leste, entretanto alterada pela Lei n.º 19/2021 de 8 de setembro, Jornal da República n.º 37 - I.ª Série, Timor-Leste.

[12] Constante do Decreto-Lei n.º 14/2022 de 6 de abril, Jornal da República n.º 15 - I.ª Série, Timor-Leste.

[13] Resolução do Conselho n.º 7/2009 de 29 de julho, Jornal da República n.º 27 - I Série, Timor-Leste.

demográficos, ou seja, os dados pessoais do mutuário conforme definição incluída no diploma (ver artigo 3.º, alínea e)), este é um exemplo interessante em como, na verdade, todas as categorias de dados poderão ser consideradas como dados pessoais, já que tornam um indivíduo "identificado ou identificável" em virtude da relação estabelecida pela inclusão simultânea no dito sistema de informação.

A este propósito, retenha-se que a Lei Indonésia faz uma distinção que o RGPD não contém. Com efeito, os dados financeiros são considerados dados pessoais de natureza específica, a par dos dados relativos à saúde, por exemplo (ver artigo 4.º). O tratamento de dados pessoais de natureza específica motivará sempre a realização de uma avaliação de impacto sobre a proteção de dados pelo responsável pelo tratamento ou da nomeação de um encarregado de proteção de dados (ver artigos 34.º, n.º 2 e 53.º, n.º 1, respetivamente).

Finalmente, a Regulamentação da Prestação de Serviços de Telecomunicações na Rede Móvel[14] qualifica, enquanto dados de identificação do utilizador, o nome, o local de residência e o número do documento de identificação, a incluir no contrato celebrado com o operador (ver artigo 3.º, n.º 3, alínea a)). Mais importante, inclui uma definição de dados de tráfego (ver artigo 7.º, n.ºs 2 e 3), abarcando os dados de faturação (o nome e a residência do utilizador, o número do cartão SIM, os números associados a este cartão relativos a comunicações efetuadas e recebidas, a identificação do serviço, data, hora e duração da chamada e tipo de tarifa cobrada) e os de informação (volume de

[14] Decreto do Governo n.º 9/2008 de 16 de abril, Jornal da República n.º 14 - I Série, Timor-Leste.

dados transmitidos, IMEI - International Mobile Equipment Identity, célula de rede em que o equipamento móvel do utilizador está localizado em determinado momento).

As finalidades e condições de legitimidade do tratamento dos dados pessoais

A mesma Regulamentação da Prestação de Serviços de Telecomunicações na Rede Móvel vem estabelecer que o operador deve tratar os dados recolhidos e gerados ao abrigo da prestação do serviço, incluindo os dados de tráfego, para os fins contratualmente estabelecidos, o que pode incluir, como finalidades para além da mera gestão do contrato, a adaptação do serviço às necessidades do utilizador, o pagamento das interligações, a operação e manutenção da rede, fins estatísticos, ações de informação ao utilizador e à autoridade reguladora, marketing/telemarketing, bem como a inclusão nas listas de assinantes (ver artigo 6.º, n.ºs 3 e 4).

Esta lista de finalidades é bem abrangente e, com efeito, inclui interesses legítimos do operador, maxime a realização de marketing/telemarketing, para além da execução do contrato ou diligências contratuais, enquanto condições de tratamento admissíveis.

O que não se encontra previsto, nem mesmo na Constituição, é o direito de oposição do utilizador (ver o artigo 21.º do RGPD, por exemplo), o qual foi previsto noutras legislações de modo a salvaguardar o titular da utilização demasiado flexível dos seus dados.

"O exercício do direito de oposição pressupõe a existência de um tratamento de dados legítimo que tenha como fundamento de legitimidade não o consentimento, nem uma obrigação legal, mas por exemplo (...) a realização de interesses legítimos do responsável pelo tratamento ou de um terceiro (...)" (Pinheiro, 2018: 385). Ora, segundo o recital 69 do RGPD, "(...) o titular não deverá deixar de ter o direito de se opor ao tratamento dos dados pessoais que digam respeito à sua situação específica. Deverá caber ao responsável pelo tratamento provar que os seus interesses legítimos imperiosos prevalecem sobre os interesses ou direitos e liberdades fundamentais do titular dos dados".

Por outro lado, a Regulamentação da Lei do Serviço Militar[15] estipula que os dados pessoais recolhidos das certidões de nascimento e preenchidos na declaração individual de recenseamento militar, os que servirão para elaborar o boletim individual de recenseamento militar, apenas poderão ser utilizados para efeitos de recenseamento militar (ver artigo 21.º, n.º 6).

O arquivo físico e digital que resulte de prestações destinadas à proteção na gravidez e encargos familiares com crianças ("Bolsa da Mãe-Nova Geração") deve, face aos dados pessoais que o componham, incluindo dados biométricos, ser apenas utilizado para a realização destas prestações[16].

Finalmente, os dados pessoais recolhidos no âmbito do levantamento cadastral, nomeadamente a identificação dos

[15] Constante do Decreto-Lei n.º 3/2021 de 13 de janeiro, Jornal da República n.º 3 - I.ª Série, Timor-Leste.

[16] Ver artigo 40.º, n.º 2 do Decreto-Lei n.º 22/2021 de 10 de novembro, Jornal da República n.º 45 - I.ª Série, Timor-Leste.

titulares cadastrais e os demais elementos cadastrais, devem ser utilizados para a composição da base cadastral e para a emissão da certidão do título de propriedade (ver artigo 36.º, n.ºs 2 e 3 do Decreto-Lei sobre Informação Cadastral Predial[17]) ou outra finalidade equivalente. Já os dados pessoais constantes da base de dados do registo predial apenas podem ser utilizados para efeitos de segurança do comércio jurídico (ou outra finalidade equivalente), nomeadamente contribuindo para uma informação organizada e atualizada sobre a situação jurídica dos prédios (ver artigo 122.º do Código de Registo Predial).

A propósito das condições de legitimidade do tratamento e sem prejuízo do que foi referido em epígrafe em matéria de necessidade de consentimento para o tratamento de dados sensíveis, apenas o consentimento expresso, por escrito, do titular legitima a divulgação dos seus dados estatísticos de caráter individual, com exceção dos dados respeitantes à atividade profissional ou empresarial, uma vez que não são alvo de segredo estatístico e poderão então constar de registos públicos nos termos legalmente aplicáveis (ver artigo 10.º, n.º 5 e 6 do Regime Jurídico do Recenseamento Geral da População e da Habitação).

Também o consentimento expresso, por escrito, é necessário à recolha e divulgação de dados pessoais constantes dos documentos oficiais previstos no Decreto-Lei com as Regras Relativas ao Acesso a Documentos Oficiais (ver artigo 16.º, n.ºs 1 e 5).

[17] Decreto-Lei n.º 65/2022 de 31 de agosto, Jornal da República n.º 35 - I.ª Série, Timor-Leste.

Finalmente, o consentimento por escrito deve ser obtido por parte dos clientes antes do envio pelas instituições de crédito dos dados de crédito ao sistema de informação de registo de crédito (ver artigo 20.º, n.º 1 da Resolução sobre o Estabelecimento do Sistema de Informação de Registo de Crédito). Existe uma minuta com uma cláusula de consentimento no respetivo Anexo I à Resolução.

Os períodos de conservação dos dados pessoais

São diversos os períodos de conservação dos dados pessoais previstos pela legislação de Timor-Leste. Assim, o Regime Jurídico da Identificação Civil inclui um prazo de conservação dos dados pessoais na base de identificação civil até cinco anos após o óbito do respetivo titular, sendo o prazo alargado para vinte anos em ficheiro histórico (ver artigo 32.º).

O Regime Jurídico do Recenseamento Geral da População e da Habitação determina que os questionários contendo dados pessoais devem ser eliminados até cinco anos após o momento censitário (ver artigo 11.º, n.º 2).

Os dados de crédito referentes a cada mutuário devem ser conservados no sistema de informação de registo de crédito por um período de tempo não inferior a cinco anos a contar da data do reembolso total do crédito. Já qualquer informação sobre atrasos de pagamento, incumprimento do contrato de mútuo ou insolvência do mutuário deve ser conservada por um período de tempo não inferior a dez anos (ver artigo 16.º, n.ºs 1 e 2 da Resolução sobre o Estabelecimento do Sistema de Informação de Registo de Crédito).

Por outro lado, as entidades abrangidas pelo Regime Jurídico de Prevenção e do Combate ao Branqueamento de Capitais e Financiamento do Terrorismo[18] devem conservar cópias dos documentos de identificação, das fichas de contas e correspondência até cinco após o fim da relação contratual, bem como qualquer informação transacional e respetivos relatórios de controlo até cinco anos após a realização da transação (ver artigo 15.º, n.º 1 alíneas a) e b)).

A Nova Lei das Sociedades Comerciais[19] determina que os livros e documentação da sociedade (ex. livros de atas), os quais podem conter dados pessoais, devem ser conservados por um período de cinco anos (ver artigos 158.º, n.º 2 e 296.º, n.º 1).

Já a propósito de impostos e taxas alfandegárias, o prazo de conservação tanto em matéria de declarações de imposto sobre vendas (ver o artigo 17.º, n.º 4 da Lei Tributária[20]) como de documentos relativos a operações aduaneiras efetuadas (ver o artigo 18.º, n.º 1 do Código Aduaneiro de Timor-Leste[21]) é de cinco anos.

Finalmente, o operador de telecomunicações em rede móvel deve manter os dados de identificação do utilizador por um período de cinco anos a contar da data de celebração do

[18] Lei n.º 17/2011 de 28 de dezembro, Jornal da República n.º 46 - I.ª Série, Timor-Leste, entretanto alterada pela Lei n.º 5/2003 de 14 de agosto, Jornal da República n.º 28 - I.ª Série, Timor-Leste.

[19] Constante da Lei n.º 10/2017 de 17 de maio, Jornal da República n.º 19 - I.ª Série, Timor-Leste.

[20] Lei n.º 8/2008 de 30 de junho, Jornal da República n.º 26 - I.ª Série, Timor-Leste, entretanto alterada pela Lei n.º 5/2019 de 27 de agosto, Jornal da República n.º 33 B - I.ª Série, Timor-Leste.

[21] Constante do Decreto-Lei n.º 14/2017 de 5 de abril, Jornal da República n.º 13 - I.ª Série, Timor-Leste.

contrato, em arquivo eletrónico ou físico (ver artigo 6.º, n.º 1 da Regulamentação da Prestação de Serviços de Telecomunicações na Rede Móvel). Os dados de tráfego devem ser conservados por um período mínimo de um ano a partir da data em que foram originados (ver artigo 7.º, n.º 4).

Os direitos dos titulares dos dados

Os titulares dos dados têm vários direitos consagrados de forma dispersa na legislação timorense. Assim, o direito de acesso encontra-se previsto no Regime Jurídico da Identificação Civil, face aos registos respeitantes, com a indicação do significado de quaisquer códigos e abreviaturas (ver artigo 30.º). O direito de acesso por terceiros é também admitido a descendentes, ascendentes, o cônjuge, tutor[22] ou curador do titular dos dados ou, em caso de falecimento deste, os presumíveis herdeiros, mediante interesse legítimo e respeitando a vida privada do titular (ver artigo 29.º, n.º 1). A Direção Nacional de Registos e Notariado (Ministério da Justiça) é a entidade responsável pela receção e resposta a estes pedidos, assegurando também o direito de acesso aos dados constantes do sistema de informação do passaporte eletrónico de Timor-Leste (ver artigo 50.º, n.º 3 do Novo Regime Jurídico dos Passaportes).

Também o direito de retificação é contemplado no Regime Jurídico da Identificação Civil (ver artigo 31.º, n.º 1) e no Novo Regime Jurídico dos Passaportes (ver artigo 50.º, n.º 3) para efeitos de correção de inexatidões, supressão de dados

[22] Atente-se, neste ponto, que a maioridade em Timor-Leste é atingida aos 17 anos (artigo 118.º do Código Civil).

incorretamente preenchidos ou de omissões. A Regulamentação da Lei do Serviço Militar estabelece o direito de alteração à informação relativa à residência, habilitações literárias e estado civil do titular dos dados que esteja na reserva de recrutamento e na reserva de disponibilidade. Este direito é exercido perante o Ministério da Defesa, que deve comunicar tais alterações ao Ministério da Justiça num prazo de sessenta dias (ver artigo 98.º).

Os eleitores têm o direito de acesso e retificação dos dados eleitorais perante o Secretariado Técnico de Administração Eleitoral (ver artigo 16.º, n.º 1 e 3 da Lei do Recenseamento Eleitoral)[23].

De igual modo, os titulares cadastrais têm o direito de acesso e de retificação dos seus dados inexatos, incompletos ou incorretamente inseridos, a exercer perante a Direção Nacional dos Serviços Cadastrais (Ministério da Justiça) (ver artigo 37.º do Decreto-Lei sobre Informação Cadastral Predial). Ademais, dispõem também do direito à informação sobre os dados pessoais que lhes dizem respeito, a sua finalidade e a identidade da entidade responsável pela base de dados (ver artigo 40.º). Não é claro se a Direção Nacional dos Serviços Cadastrais presta esta informação via política de privacidade ou outra forma, mas tal dever compete-lhe nos moldes atrás expostos.

Idênticos direitos de acesso, retificação e de informação (incluindo também o endereço da entidade responsável pela base de dados) encontram-se consagrados a favor dos titulares do registo predial, a exercer perante o Diretor Nacional de Registos e

[23] Este diploma enquadra também o apagamento de dados em caso de óbito do eleitor, embora tal não resulte do exercício de um direito (ver artigos 14.º e 16.º, n.º 3).

Notariado (ver artigos 123.º, n.º 2 e 128.º do Código de Registo Predial).

Finalmente, os mutuários têm direito de acesso e retificação dos seus dados de crédito. O direito de acesso deve ser respondido por escrito pela Autoridade Bancária e de Pagamentos num prazo de 10 dias úteis a contar da data de receção do pedido. O primeiro pedido em cada ano é respondido gratuitamente, sendo os demais pedidos sujeitos a uma taxa administrativa (ver artigo 19.º da Resolução sobre o Estabelecimento do Sistema de Informação de Registo de Crédito). O direito de retificação pode ser exercido face à instituição de crédito ou à Autoridade Bancária e de Pagamentos, devendo a correção reportar-se apenas aos factos verificados no momento da inserção no sistema de informação de registo de crédito. Não pode haver correção de informação adversa devido a cumprimento posterior ou alteração das circunstâncias do mutuário (ver artigo 12.º, n.º 2 a 5).

No que diz respeito ao catálogo de direitos do RGPD, este é mais alargado do que aquele constante na legislação timorense, a qual poderá ser enriquecida com base neste(s) exemplo(s).

O RGPD prevê, para além do direito à informação (ver artigos 13.º e 14.º), do direito de acesso (ver artigo 15.º) e do direito de retificação (ver artigo 16.º); o direito ao apagamento dos dados pessoais do titular em determinadas circunstâncias (ver artigo 17.º); o direito à limitação do tratamento também em determinadas circunstâncias (ver artigo 18.º); o direito de portabilidade dos dados, em uso corrente e de leitura automática, e da sua transmissão a outro responsável pelo tratamento (ver artigo 20.º); o direito de oposição, melhor explicado acima (ver

artigo 21.º); e o direito de não sujeição a decisões exclusivamente automatizadas, incluindo a definição de perfis, que possam produzir efeitos na esfera jurídica ou afetar significativamente os titulares dos dados (ver artigo 22.º).

O RGPD, para além de esclarecer o conteúdo de cada direito e as limitações aplicáveis, consagra perante quem deve ser exercido e os prazos eventualmente aplicáveis (ver, a este propósito, o artigo 12.º). Nomeadamente, o exercício de todos os direitos deve ser facilitado pelo responsável do tratamento (salvo se não for possível identificar o titular ou se o exercício for repetitivo e sem justificação); tal exercício deverá ser gratuito (a menos que seja manifestamente infundado ou excessivo) e a resposta aos direitos de acesso, retificação, apagamento, limitação e portabilidade deverá ocorrer no prazo de um mês a contar da data de receção do pedido, com possibilidade de prorrogação até dois meses, atendendo à complexidade e número de pedidos.

Quanto à Lei Indonésia, o catálogo de direitos é relativamente idêntico ao catálogo de direitos constante do RGPD (ver artigos 5.º a 13.º)[24]. Destaca-se, porém, o prazo bastante mais apertado de resposta ao exercício dos direitos de acesso, limitação e oposição por parte do responsável pelo tratamento - este disporá apenas de setenta e duas horas para

[24] O direito de indemnização do titular dos dados está elencado no capítulo da Lei Indonésia referente aos direitos (ver artigo 12.º), ao passo que no RGPD se encontra apenas previsto no capítulo sobre vias de recurso, responsabilidade e sanções (ver artigo 82.º).

atender à solicitação do titular dos dados (ver artigos 32.º e 41.º)[25].

A segurança dos dados pessoais

A ideia de segurança dos dados pessoais encontra eco, antes de mais, na legislação relativa a documentos de identificação. A base de dados de identificação civil deve conter as medidas de segurança próprias para impedir a consulta, a modificação, a supressão, a adição, a destruição ou a comunicação de dados por forma não consentida.

O artigo 32.º do Regime Jurídico da Identificação Civil pormenoriza que o acesso e introdução de dados pessoais em sistemas de tratamento automatizado só pode ocorrer por pessoas autorizadas, no âmbito das suas atribuições legais, devendo ser possível verificar quais foram as informações introduzidas, quando e por quem. A transmissão e o armazenamento de dados devem ser efetuados por forma a impedir qualquer leitura, cópia, alteração ou eliminação não autorizadas[26]. Finalmente, a interconexão dos dados existentes na base de dados de identificação não é admissível nos termos gerais (ver artigo 27.º, n.º 2).

Já o sistema de informação do passaporte eletrónico de Timor-Leste deve reger-se pelos princípios da segurança e do controlo da informação, assegurando níveis de acesso, de

[25] O responsável pelo tratamento também dispõe apenas de setenta e duas horas para pôr termo ao tratamento em caso de retirada do consentimento (ver artigo 40.º).

[26] A Lei do Recenseamento Eleitoral inclui medidas de segurança similares no seu artigo 19.º.

modificação, de adicionamento ou de supressão de dados, bem como formas de comunicação daqueles (ver artigo 49.º, n.º 2 do Novo Regime Jurídico dos Passaportes). Futuras especificações técnicas serão alvo de legislação própria (ver artigo 50.º, n.º 2).

A base de dados cadastral, de acordo com o artigo 38.º, n.º 1 do Decreto-Lei sobre Informação Cadastral Predial, deve ser gerida de modo a garantir a respetiva confidencialidade, integridade e autenticidade, nomeadamente ao registar as consultas efetuadas e ao delimitar o universo dos utilizadores. Também a base de dados do registo predial deve controlar as pesquisas efetuadas e ser subordinada a níveis de acesso atualizados, impedindo então a consulta, modificação, supressão, o acrescentamento ou a comunicação não autorizados de dados (ver 129.º do Código de Registo Predial).

Em matéria de operadores de telecomunicações móveis, os dados recolhidos devem ser tratados com adequadas condições de segurança, sob pena de responsabilidade nos termos legalmente aplicáveis (ver artigo 6.º, n.º 3 da Regulamentação da Prestação de Serviços de Telecomunicações na Rede Móvel). Finalmente, as instituições de crédito são obrigadas a investigar as falhas de privacidade e segurança em sistemas informáticos e a relatar o resultado das investigações e as medidas de mitigação adotadas à Autoridade Bancária e de Pagamentos (ver ponto 8 do Contrato de Partilha de Informação de Crédito, incluído enquanto Anexo 2 da Resolução que estabelece o Sistema de Informação de Registo de Crédito).

Uma futura legislação timorense de proteção dos dados pessoais incluirá seguramente disposições mais detalhadas sobre medidas de segurança de informação. Na esteira do

RGPD, poderá elencar sumariamente as medidas técnicas e organizativas adequadas, por exemplo, a pseudonimização e a cifragem, bem como a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento (ver artigo 32.º, n.º 1, alíneas a) e b)).

De forma semelhante, a Lei Indonésia prevê também que o responsável pelo tratamento deve determinar o nível de proteção dos dados pessoais, estabelecendo medidas de segurança consoante o risco[27] (ver artigo 35.º).

Por outro lado, o que ambas as legislações preveem é a necessidade de reporte de qualquer incidente de segurança que motive uma violação de dados pessoais, ou seja, "(...) de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento" (ver artigo 4.º, n.º 12 do RGPD).

A diferença interessante neste aspeto é que, embora o RGPD e a Lei Indonésia estabeleçam a necessidade de notificação num prazo máximo de sessenta e duas horas após conhecimento da ocorrência e incluindo informação sobre a natureza da violação, os dados pessoais abrangidos e as medidas adotadas; aquelas leis divergem em matéria dos destinatários de cada notificação.

[27] Esta noção de risco é bem evidente no RGPD. Exemplificativamente, leia-se o recital 76: "A probabilidade e a gravidade dos riscos para os direitos e liberdades do titular dos dados deverá ser determinada por referência à natureza, âmbito, contexto e finalidades do tratamento de dados. Os riscos deverão ser aferidos com base numa avaliação objetiva, que determine se as operações de tratamento de dados implicam risco ou risco elevado".

Assim, o RGPD estabelece que uma autoridade de controlo deve ser notificada sempre que haja risco para os direitos e liberdades de pessoas singulares e os titulares dos dados apenas carecem de notificação em caso de risco elevado (ver artigos 33.º, n.º 1 e 34.º, n.º 1 do RGPD)[28].

Já a Lei Indonésia estabelece a obrigatoriedade de notificação tanto à autoridade de controlo como aos titulares dos dados em qualquer situação de violação (logo, independentemente do risco), bem como ao público em geral em determinadas circunstâncias a estabelecer futuramente (ver artigo 46.º). A este regime mais exigente não será alheia a sucessão de casos de violação de dados pessoais na Indonésia que motivaram, aliás, a redação desta Lei[29].

As técnicas de pseudonimização/anonimização dos dados pessoais

Ainda que de forma ténue, existem algumas referências a técnicas de agregação de dados pessoais, de modo que estes

[28] O tópico da violação de dados pessoais suscitou a emissão de diferentes orientações pelo Comité Europeu para a Proteção de Dados, organismo europeu independente que contribui para a aplicação coerente de regras em matéria de proteção de dados na União Europeia (ver artigo 68.º e seguintes do RGPD). Assim, as Orientações 01/2021, com exemplos relativos à notificação de violações de dados pessoais, foram adotadas a 14 de dezembro de 2021 (versão 2.0, após consulta pública); e as Orientações 9/2022, sobre a notificação de violações de dados pessoais no âmbito do RGPD foram adotadas a 10 de outubro de 2022 e encontram-se presentemente em fase de consulta pública.

[29] A este respeito, Timmerman, Antonia (5 outubro 2022), "Sick of data leaks, Indonesians are siding with a hacker who exposed 1.3 billion SIM card details", in *Rest of World* [em linha], [consultado em 8 de novembro de 2022] disponível em https://restofworld.org/2022/indonesia-hacked-sim-bjorka/.

possam ser divulgados sem causarem a respetiva identificação dos titulares.

O Regime Jurídico da Identificação Civil admite a autorização de acesso a dados de identificação civil, desde que as pessoas a que respeitem não sejam identificáveis, para fins de investigação científica ou de estatística (ver artigo 29.º, n.º 2). Também a Lei do Recenseamento Eleitoral autoriza a divulgação de dados para fins estatísticos e de relevante interesse público, desde que tenham sido anonimizados (ver artigo 18.º). De igual modo, o Decreto-Lei sobre a Informação Cadastral Predial contempla a cedência de informação para fins de investigação estatística e de elaboração de estatísticas desde que os titulares cadastrais não se encontrem identificados (ver artigo 39.º, n.º 5)[30].

O Regime Jurídico do Recenseamento Geral da População e da Habitação prevê que os dados pessoais recolhidos nos questionários são tornados anónimos quando transpostos para suporte informático (ver artigo 11.º, n.º 3), preservando então o segredo estatístico.

Finalmente, a Resolução que estabelece o Sistema de Informação de Registo de Crédito avança com a possibilidade de revelação, pela Autoridade Bancária e de Pagamentos, de dados de crédito de forma consolidada para efeitos estatísticos, ou seja, sem expor a identidade de cada mutuário (ver artigo 23.º).

Conforme referido acima, o recital 26 do RGPD, que considera que os dados pseudonimizados estão sujeitos à sua aplicação, também esclarece que os dados anónimos se

[30] Disposição idêntica encontra-se no artigo 126.º, n.º 5 do Código de Registo Predial.

encontram subtraídos ao seu regime legal, inclusive para efeitos estatísticos ou de investigação. Todavia, tal regime de exceção também motiva a existência de dados apenas ilusoriamente anonimizados, fruto da evolução crescente das tendências computacionais que permitem a reidentificação num cada vez maior número de situações, logo uma vulnerabilização progressiva dos titulares dos dados[31]. Será conveniente que tal ponderação seja incorporada na futura lei de proteção dos dados pessoais de Timor-Leste.

As situações de transmissão dos dados pessoais

Quais são as situações de transmissão dos pessoais consagradas na legislação de Timor-Leste?

Por exemplo, a Direção Nacional de Registos e Notariado assegura a transmissão de dados de identificação civil às entidades policiais e judiciárias, segundo pedido fundamentado e apenas para fins de investigação ou de instrução criminal (ver artigos 26.º, n.º 1 e 2, e 28.º, n.º 1 do Regime Jurídico da Identificação Civil).

A mesma Direção Nacional de Registos e Notariado comunica dados sobre passaportes ao Departamento de Migração e à Direção de Assuntos Consulares (ver artigo 51.º, n.º 1 do Novo Regime Jurídico dos Passaportes).

Também os dados pessoais constantes da base de dados cadastral podem ser comunicados ou facilitado o acesso direto à aplicação informática que gere e trata do cadastro, com respeito

[31] Ver Torbay, Augusto Cesar (2020). A anonimização enquanto mecanismo de proteção de dados pessoais à luz da atual conjuntura legislativa europeia. *Anuário da Proteção de Dados*, 2020: 49-78.

pelas regras de segurança de informação, face aos organismos e serviços do Estado, nomeadamente tribunais, serviços de registo predial, cartórios notariais, administração fiscal, planeamento urbano e ordenamento do território mas apenas para a prossecução das respetivas atribuições e competências (ver artigo 39.º, n.º 2 e 3 do Decreto-Lei sobre Informação Cadastral Predial). Disposição idêntica encontra-se prevista nos artigos 126.º, n.º 2 e 127.º, n.º 1 do Código de Registo Predial, beneficiando magistrados judiciais e do Ministério Público, bem como entidades competentes em matéria de segurança interna.

Para efeitos de verificação de identificação, eliminação de inscrições indevidas e correção de outras irregularidades, pode haver cruzamento da base de dados de recenseamento eleitoral com as bases de dados do Ministério da Justiça, do Ministério da Solidariedade Social e com o Ministério dos Negócios Estrangeiros e da Cooperação (ver artigo 15.º da Lei do Recenseamento Eleitoral). Igual comunicação dos dados eleitorais pode ocorrer com forças de segurança e serviços e organismos da Administração Pública, no âmbito da prossecução das suas competências e quando isso não se manifeste incompatível com a finalidade que presidiu à recolha dos dados eleitorais (ver artigo 17.º).

De igual modo, a Comissão Anti-Corrupção ou o Supremo Tribunal de Justiça podem ter acesso a bases de dados (ex. registo civil, registo automóvel, registo de propriedades e de sociedades comerciais) para verificação das declarações de

rendimentos, bens e interesses no âmbito das Medidas de Prevenção e Combate à Corrupção[32].

Já os dados estatísticos de caráter individual recolhidos em cada recenseamento, sendo de natureza confidencial e não podendo à partida ser fornecidos a quaisquer pessoas ou entidades, podem ser transmitidos à Direção-Geral de Impostos e a outras entidades para efeitos de investigação científica, mas apenas mediante diploma próprio do Governo (ver artigo 10.º, n.º 3 do Regime Jurídico do Recenseamento Geral da População e da Habitação).

Finalmente, o operador de telecomunicações móveis deve comunicar dados de tráfego no âmbito de processo judicial, desde que este pedido se mostre individualizado e suficientemente concretizado, com autorização do juiz competente; bem como deve informar mensalmente a Autoridade Reguladora das Comunicações sobre os utilizadores que tenham utilizado indevidamente, cometido fraude ou falsificado o cartão SIM, divulgando nome completo e número de identificação (ver artigos 8.º e 9.º da Regulamentação da Prestação de Serviços de Telecomunicações na Rede Móvel).

Em especial, as transferências internacionais dos dados pessoais

Numa economia digital globalizada, um dos seus aspetos relevantes passa pela possibilidade de transferir dados entre países. Contudo, tais transferências não devem esvaziar as garantias dos titulares dos dados. No que diz respeito à União

[32] Lei n.º 7/2020 de 26 de agosto, Jornal da República n.º 35 - I.ª Série, Timor-Leste

Europeia, por exemplo, "(...) o legislador da União, visando o justo equilíbrio entre os valores públicos e os interesses particulares em apreço, sempre teve a preocupação de balancear o princípio da livre circulação das pessoas e dos seus dados (...) e a proteção dos direitos e liberdade fundamentais, nomeadamente a proteção da privacidade e dos dados pessoais" (Oliveira, Inês, 2018: p. 87).

Neste contexto, e não dispondo Timor-Leste de qualquer norma sobre transferências internacionais de dados, vejamos quais são as disposições vigentes nos nossos dois casos de análise.

O RGPD inclui um capítulo próprio sobre transferências de dados para países terceiros ou organizações internacionais. Como princípio geral, qualquer transferência de dados pessoais só poderá ocorrer se o nível de proteção das pessoas singulares não for comprometido (ver artigo 44.º). Semelhante nível de proteção poderá ser garantido através de uma decisão de adequação atribuída a determinados Estados (ver artigo 45.º)[33] [34], da celebração de cláusulas-tipo adotadas pela Comissão ou pela autoridade de controlo (ver artigo 46.º), de regras vinculativas aplicáveis às empresas conforme aprovadas pela autoridade de

[33] A lista de países que beneficiam atualmente de uma decisão de adequação segundo o artigo 45.º do RGPD encontra-se disponível através de https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, consultado em 6 de novembro de 2022.

[34] A este propósito, sobre as transferências de dados pessoais entre a União Europeia e os E.U.A.. não deve ser esquecida a invalidação sucessiva dos International Safe Harbor Privacy Principles e do EU-US Privacy Shield pelo Tribunal de Justiça da União Europeia, em 2015 e 2020, respetivamente (casos Schrems I e Schrems II). Atualmente, ambas as partes anunciaram a Trans-Atlantic Data Privacy Framework; a Presidência americana já assinou a ordem executiva para a sua implementação, mas o processo de ratificação pela Comissão Europeia ainda se encontra em curso.

controlo (ver artigo 47.º) ou de determinadas derrogações como o consentimento expresso pelo titular (ver artigo 49.º).

A Lei Indonésia prevê a possibilidade de transferências de dados para países terceiros em três situações: a) quando o país terceiro beneficie de um nível de proteção de dados pessoais equivalente ou inclusive mais elevado; b) se a condição anterior não se verificar, a transferência pode ainda assim ocorrer caso o responsável pelo tratamento garanta, de forma adequada e segundo o caso concreto, que os dados pessoais serão tratados consoante as disposições da Lei Indonésia; c) se as duas condições anteriores não se verificarem, o responsável pelo tratamento deverá obter o consentimento do titular de modo a realizar a transferência (ver artigo 56.º).

A Indonésia é um dos países-membros da Associação das Nações do Sudeste Asiático ("ASEAN" enquanto acrónimo em língua inglesa)[35]. Na cimeira da ASEAN realizada no Camboja em novembro de 2022, Timor-Leste foi considerado enquanto futuro 11.º membro pelos demais Estados, sendo admitido como membro observador em todas as reuniões e cimeiras da ASEAN.

A ASEAN dispõe de um "Enquadramento sobre Proteção de Dados Pessoais"[36], aprovado em 2016. Este Enquadramento baseia-se numa lista de princípios, nomeadamente: a) Consentimento, notificação e finalidade; b) Rigor dos dados pessoais; c) Garantias de segurança; d) Acesso e retificação; e)

[35] A lista de países-membros é atualmente composta por Brunei Darussalam, Camboja, Filipinas, Indonésia, Malásia, Myanmar, República Democrática Popular do Laos, Singapura, Tailândia e Vietname. Destes países, apenas as Filipinas, a Indonésia, Malásia, Singapura e Tailândia dispõem de leis gerais de proteção de dados.

[36] Disponível através de https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf, consultado em 6 de novembro de 2022.

Transferências para outro país ou território; f) Conservação; g) Responsabilização.

Ora, em matéria de transferências internacionais de dados, a ASEAN aprovou um modelo de cláusulas-tipo[37] em 2021, aplicável a relações entre um responsável pelo tratamento e um subcontratante (quem trata os dados pessoais por conta do responsável pelo tratamento) e a relações entre dois responsáveis pelo tratamento. Este modelo de cláusulas-tipo pode ser adotado voluntariamente por entidades privadas sediadas em países da ASEAN, a par de outros mecanismos legitimadores de transferências internacionais de dados. Semelhante adoção não preclude a necessidade de cumprimento da legislação vigente no respetivo país exportador de dados. A este propósito, veja-se o caso de Singapura, que adotou um "Guia de Utilização das Cláusulas-Contratuais Tipo da ASEAN para Fluxos Transfronteiriços de Dados desde Singapura"[38].

As sanções

Para além do crime de violação de segredo, previsto no artigo 184.º do Código Penal[39], o qual visará qualquer indivíduo que viole o dever de segredo e confidencialidade previsto em muitos dos diplomas acima analisados a propósito da proteção

[37] Disponível através de https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf, consultado em 6 de novembro de 2022.

[38] Disponível através de https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Singapore-Guidance-for-Use-of-ASEAN-MCCs.pdf?la=en, consultado em 6 de novembro de 2022.

[39] Aprovado pelo Decreto-Lei n.º 19/2009 de 8 de abril, Jornal da República n.º 14 - I.ª Série, Timor-Leste, entretanto ultimamente alterado pela Lei n.º 5/2017 de 19 de abril, Jornal da República n.º 15 - I.ª Série, Timor-Leste.

dos dados pessoais (a título de exemplo, ver artigo 21.º do Regime Jurídico do Recenseamento Geral da População e da Habitação), o Decreto-Lei com as Regras Relativas ao Acesso a Documentos Oficiais estabelece contraordenações a respeito da recolha indevida de dados pessoais.

Assim, sempre que os dados pessoais constantes de documentos oficiais sejam recolhidos sem autorização expressa do titular ou por alguém que não seja um profissional devidamente autorizado/certificado (ver artigo 16.º, n.ºs 1 e 2), a coima aplicável é de 300 a 5.000 dólares, tratando-se de pessoa singular, ou de 700 a 30.000 dólares, tratando-se de pessoa coletiva (ver artigo 14.º, n.º 1, alínea e) e n.º 2).

Em jeito de comparação, veja-se que a Lei de execução Portuguesa prevê, em caso de acesso indevido aos dados pessoais, sem a devida autorização ou justificação, uma pena de prisão de 1 ano ou uma pena de multa até 120 dias (ver artigo 47.º, n.º 1). A pena é, porém, agravada para o dobro nos seus limites quando: a) o acesso seja referente a categorias especiais de dados ou dados relacionados com condenações penais ou infrações; b) for conseguido através da violação de regras técnicas de segurança; c) tiver proporcionado ao agente ou a terceiros benefício ou vantagem patrimonial (ver n.ºs 2 e 3 do mesmo artigo). Uma pessoa coletiva também poderá ser responsabilizada nos termos do artigo 11.º do Código Penal Português.

Na Lei Indonésia, a recolha indevida de dados pessoais, desde que praticada conscientemente e com o propósito de obtenção de benefício próprio ou para terceiros, resultando também em prejuízo para os titulares dos dados, é punida com

pena de prisão até 5 anos ou pena de multa até 5 milhões de rúpias (ver artigo 67.º, n.º 1). Se o crime for cometido por uma pessoa coletiva, a pena de multa será até 50 milhões de rúpias.

Conclusão

A ausência de uma lei própria de proteção dos dados pessoais não significa que o legislador timorense não tenha tratado desta matéria em diversas leis, como este texto bem demonstra. Assim, a par da Constituição, a legislação ordinária de Timor-Leste inclui disposições sobre as categorias de dados pessoais, sobre condições de legitimidade de tratamento e respetivas finalidades, sobre períodos de conservação, sobre direitos dos titulares dos dados, sobre segurança dos dados pessoais, sobre pseudonimização e anonimização, sobre transmissão de dados e até sobre sanções relativas a este tópico.

O que falta agora é uma lei geral que concretize a definição de dados pessoais, incluindo os dados sensíveis, que esclareça as condições de legitimidade de tratamento, que expanda o catálogo de direitos e conforme as regras de exercício, que clarifique as obrigações do responsável pelo tratamento e do subcontratante, que regule as transferências internacionais de dados (em articulação com a adesão à ASEAN), que crie uma autoridade de controlo e que estabeleça o regime de responsabilidade e sanções, incluindo as vias de recurso.

Ao longo deste texto, utilizei o RGPD e a Lei Indonésia para efeitos de comparação, de modo a aprofundar a reflexão sobre as disposições existentes na legislação timorense. Talvez tal

exercício de direito comparado também possa ser realizado a propósito da redação da futura lei de proteção dos dados pessoais.

Finalmente, a aprovação de uma lei geral também poderá ser uma oportunidade de reflexão sobre eventuais inconsistências do ordenamento jurídico vigente. Por exemplo, serão todas as situações de transmissão de dados pessoais entre entidades públicas, conforme descritas no capítulo acima subordinado ao tema, consentâneas com as finalidades que presidiram à recolha dos respetivos dados alvo de transmissão? Fica a sugestão de análise.

Qual a verdadeira importância de uma lei de proteção dos dados pessoais? Bem, antes de mais, fomenta a confiança nas entidades públicas e privadas que detêm os nossos dados e isso facilita o comércio jurídico. Aumenta o controlo sobre os nossos dados pessoais e isso protege a nossa reputação. Facilita a liberdade de expressão e o envolvimento na esfera pública. Cria instrumentos para regular as circunstâncias em que os nossos dados pessoais são tratados e a possibilidade de responsabilizar quem utiliza ou acede a tais dados indevidamente, incluindo casos de violação de dados pessoais. As vantagens são inúmeras e, no mundo atual, ter uma lei de proteção dos dados pessoais em vigor significa também que o respetivo Estado está a par da sua relevância.

Que Timor-Leste dê esse passo o mais brevemente possível.

Bibliografia

Livros

Cordeiro, António Menezes (reimpressão 2022). Direito da Proteção de Dados à luz do RGPD e da Lei n.º 58/2019. Coimbra: Almedina;

Miranda, Jorge e Medeiros, Rui (2017). Constituição Portuguesa Anotada, Tomo I. Lisboa: Universidade Católica Editora;

Pinheiro, Alexandre Sousa (Coord.), Coelho, Cristina Pimenta et al. (2018). Comentário ao Regulamento Geral de Proteção de Dados. Coimbra: Almedina.

Artigos de publicações periódicas

Solove, Daniel J. (2013). Introduction: Privacy Self-Management and the Consent Dilemma. Harvard Law Review. Volume 126: 1880-1903;

Oliveira, Inês (2018). O direito à proteção de dados pessoais e o regime jurídico das transferências internacionais de dados: a proteção viaja com as informações que nos dizem respeito?. Anuário da Proteção de Dados, 2018: 71-90;

Torbay, Augusto Cesar (2020). A anonimização enquanto mecanismo de proteção de dados pessoais à luz da atual conjuntura legislativa europeia. Anuário da Proteção de Dados, 2020: 49-78.

Sítios web na Internet

Ke, Xu et al. (24 agosto 2021). Analyzing China's PIPL and how it compares to the EU's GDPR. In The Privacy Advisor [em linha]. [consultado em 14 de outubro de 2022]. Disponível em https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/;

Timmerman, Antonia (5 outubro 2022). Sick of data leaks, Indonesians are siding with a hacker who exposed 1.3 billion SIM card details". In Rest of World [em linha]. [consultado em 8 de novembro de 2022]. disponível em https://restofworld.org/2022/indonesia-hacked-sim-bjorka/.