REVISTA DE DIREITO ADMINISTRATIVO

JANEIRO > ABRIL '25

#22

AAFDL EDITORA

O crime de desvio de dados: contributos para uma interpretação razoável

Tiago Félix da Costa
Mestre e Advogado

Sumário: **1.** Nota Introdutória; **2.** Breve caracterização do crime de desvio de dados; **3.** O desvio de dados e as condições de licitude de tratamento de dados pessoais; **4.** O Consentimento do artigo 48.º da LPD.

1. Nota Introdutória

O *crime de desvio de dados* está consagrado no artigo 48.º da Lei n.º 58/2019, de 8 de agosto, também designada Lei da Proteção de Dados Pessoas (doravante "LPD"), que procedeu à concretização de alguns aspetos do Regulamento (UE) n.º 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, *relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados* (doravante "RGPD")[1]. Com efeito, o RGPD, além das condutas que pretendeu punir através dos seus artigos 79.º a 83.º, instou ainda os Estados-Membros a prever outras sanções, de natureza penal ou administrativa (em particular, Considerandos § 149 e 152). É nessa senda que se enquadra este crime de desvio de dados e os demais crimes da LPD, renovando-se, por essa via, o quadro criminal outrora previsto nos artigos 43.º a 4.º da anterior Lei n.º 67/98, de 26 de outubro.

Ao contrário do que sucedeu com outras normas da então Proposta de Lei 120/XIII, o artigo 48.º não gerou particular polémica ou preocupação[2], sendo certo que a sua redação permaneceu inalterada até à publicação final da LPD. Contudo, uma parte do segmento típico da norma do n.º 1 do artigo 48.º suscita dúvidas quanto à sua interpretação e, por consequência, quanto à delimitação da infração típica, o que pode causar embaraço ao comércio jurídico e à vida das organizações *responsáveis* pelo tratamento de dados pessoais[3].

Na verdade, ao prever que "*Quem copiar, subtrair, ceder ou transferir, a título oneroso ou gratuito, dados pessoais sem previsão legal ou consentimento, independentemente da finalidade prosseguida, é punido com pena de prisão até 1 ano ou com pena*

[1] O RGPD passou a disponibilizar, desde a sua entrada em vigor em 25 de maio de 2018, um conjunto único de regras diretamente aplicáveis nos Estados-Membros. Isto significa que, desde essa data, o RGPD é aplicável independentemente de quaisquer medidas concretamente definidas nas ordens jurídicas internas. Em consequência, as disposições do RGPD podem, regra geral, ser invocadas diretamente por cidadãos, empresas, administrações públicas e outras entidades que tratem dados pessoais. Sem prejuízo, os Estados-Membros procederam a uma adaptação da respetiva legislação, revogando ou alterando leis, contando ainda com liberdade para especificar as normas de proteção de dados a certos setores ou domínios, como o setor público, medicina preventiva ou do trabalho e obrigações de sigilo. Para mais desenvolvimentos a respeito da natureza e da aplicabilidade direta do RGPD, veja-se a Comunicação da Comissão ao Parlamento Europeu e ao Conselho "*Maior proteção, novas oportunidades – Orientações da Comissão relativas à aplicação direta do Regulamento Geral sobre a Proteção de Dados a partir de 25 de maio de 2018*" disponível em https://eur-lex.europa.eu/.

[2] *Vide*, por exemplo, os comentários da Comissão Nacional da Proteção de Dados à Proposta de Lei 120/XIII, no Parecer 20/2018, acessível www.parlamento.pt e, também, a Decisão 2019/494, acessível em www.cnpd.pt pela qual aquela Comissão declarou não aplicar certas normas da LPD por entender que as mesmas violam o RGPD.

[3] Nos termos do artigo 4.º, 7), do RGPD, responsável pelo tratamento será "(...) *a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro*".

de multa até 120 dias", o legislador gerou a dúvida em torno de saber quando é que a cópia, a subtração, a cedência ou a transmissão de dados pessoais fazem o respetivo agente incorrer na prática do crime de desvio de dados.

Como é fácil de compreender, enquanto formas de tratamento de dados pessoais[4] estas operações são perfeitamente banais e recorrentes na vida de qualquer organização – seguramente será o caso da cópia, da cedência e da transferência de dados pessoais –, sendo, por isso, imprescindível compreender em que casos aquelas operações são aptas a preencher o tipo do crime de desvio de dados.

À primeira vista, a resposta, apoiada no texto da norma, encontrar-se-ia nas operações realizadas sem *previsão legal* ou *consentimento* dos titulares dos dados, independentemente do seu carácter gratuito ou oneroso. Mas a questão está justamente em saber o que são "previsão legal" e "consentimento" para efeitos de verificação do elemento objetivo deste tipo de crime.

Note-se, por um lado, que *previsão legal* é um conceito estranho, nesta concreta terminologia, entre as normas de proteção de dados pessoais e, por outro, pese embora o *consentimento* seja um conceito essencial no domínio da proteção de dados, suscita-se a dúvida de saber se o consentimento do artigo 48.º da LPD é um consentimento alinhado com os requisitos que o consentimento do titular dos dados pessoais assume nas normas do RGPD – entre os quais se destaca a obrigação de o consentimento ser explícito, informado e específico – ou se, pelo contrário, é um consentimento em sentido penal, que, nos termos do artigo 39.º do Código Penal (doravante "CP"), pode até ser presumido.

Sem prejuízo de outras que afloraremos, são estas as dúvidas essenciais que a formulação atual do crime de desvio de dados nos suscita e que, ainda que de forma necessariamente sumária e incompleta, procuraremos deslindar a bem de uma interpretação razoável.

2. Breve caracterização do crime de desvio de dados

Quanto ao grau de lesão do bem jurídico, o crime de desvio de dados é um crime de perigo abstrato e, pelo menos no que respeita a algumas das suas modalidades típicas, quanto à forma de consumação do ataque ao objeto da ação, um crime de mera atividade, sendo evidente que, a par de outros crimes previstos na lei de proteção de dados, o bem jurídico protegido é a privacidade e a autodeterminação informacional[5]. Trata-se de um crime doloso, admitindo todas as modalidades de dolo, mas não se prevendo nenhum elemento subjetivo especial[6][7].

Temos dúvidas sobre a qualificação do crime como crime específico próprio[8], na medida em que, ao contrário do que sucedia na norma do artigo 43.º, n.º 1, al. c), da Lei n.º 67/98, de 26 de outubro, que punia com pena de prisão até um ano ou cento e vinte dias de multa quem *"Desviar ou utilizar dados pessoais, de forma incompatível com a finalidade determinante da recolha ou com o instrumento de legalização"* e que pressupunha necessariamente a qualidade de *responsável* pelo tratamento dados do agente, pelo menos, quanto à modalidade da *utilização* dos dados pessoais, o legislador da nova LPD operou uma distinção evidente entre estes comportamentos típicos, estabelecendo como tipos autónomos a *utilização incompatível com a finalidade da recolha*[9] (*Cfr.* artigo

---

[4] O artigo 4.º, 2), do RGPD, define tratamento de dados pessoais como "(...) *uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição*".

[5] Pedro Verdelho, em anotação ao artigo 43.º da Lei 67/98, de 26 de outubro, referia que *"Essas regras e obrigações são muito diversas e tornam por isso o interesse protegido pelo crime muito complexo"*, *Cfr. Comentário das Leis Penais Extravagantes*, Coord. Paulo Pinto de Albuquerque e José Branco, UCE, 2010, p.439.

[6] Em sentido contrário, quanto à forma de consumação do crime, Tiago Geraldo *in Comentário ao Regulamento Geral de Proteção de dados e à Lei n.º 58/2009*, coord. António Barreto Menezes Cordeiro, Almedina, 2021, pp. 655-656.

[7] Em sentido contrário, ainda que sobre o artigo 43.º, n.º 1, alínea c), da Lei n.º 67/98, de 26 de outubro, veja-se o Acórdão do Tribunal da Relação de Évora, de 26 de setembro de 2023, proferido no Processo 1044/18.1T9EVR.E1, acessível em www.dgsi.pt

[8] Qualificando o crime de desvio de dados como específico próprio, em parte, Tiago Geraldo, *ob. loc. cit.* Em sentido contrário, Pedro Dias Venâncio, in *Lições de Direito do Cibercrime e da Tutela Penal de Dados Pessoais*, Editora D'Ideias, 1.ª Ed., 2022, p. 154.

[9] Cremos que o crime do artigo 46.º da LPD é efetivamente um crime específico próprio, uma vez que a utilização dos dados pessoais para uma finalidade incompatível com a finalidade que determinou a recolha dos dados pressupõe, à luz das normas do RGPD, que o responsável pelo tratamento recolhe e trata os dados pessoais para finalidades determinadas, legítimas e explícitas e que, posteriormente, por sua determinação, lhes dá uma utilização distinta e incompatível com a finalidade inicial, nos termos e para os efeitos do disposto no artigo 5.º, n. 1.º, al. b), do RGPD. Aliás, o artigo 5.º, n. 2, esclarece que é o responsável que fica obrigado a cumprir as normas do n.º 1 do artigo 5.º do RGPD. Note-se, ainda, que, nos

46.º da LPD), que pressupõe a qualidade de responsável pelo tratamento – quem trata legitimamente os dados pessoais para uma finalidade determinada e lhes dá uma utilização incompatível com a finalidade da recolha (princípio da finalidade) –, o *acesso indevido* (*Cfr.* artigo 47.º da LPD) e o *desvio de dados* (*Cfr.* artigo 48. da LPD).

Ao contrário do que sucede no *crime de utilização de dados de forma incompatível com a finalidade da recolha* que, por referência aos princípios da finalidade e da licitude, são tratados por quem determinou as finalidades e os meios de tratamento, com base numa condição de licitude válida, e que, posteriormente, passa a tratar os dados para uma finalidade incompatível com aquela que determinou a recolha, não vemos que o *crime de desvio de dados* exija uma especial qualidade do agente, podendo as condutas típicas ser praticadas pelo responsável pelo tratamento, pelos seus colaboradores ou por terceiros[10]. Interpretação diversa, no sentido de se tratar de um crime específico próprio, poderia significar que o agente, pessoa singular, que desviasse dados pessoais para os seus próprios fins – como sucede amiúde com o *hacking* – não pudesse ser punido, o que não parece corresponder à vontade do legislador, nem encontrar suporte restritivo na interpretação semântica do enunciado desta disposição legal. Note-se, aliás, que existe já um precedente de aplicação deste ilícito típico de desvio de dados a pessoas sem a função de responsável de tratamento de dados, concretamente no Acórdão do Supremo Tribunal de Justiça n.º 225/20.2TELBS.S1, de 23 de junho de 2022, relatado pela Juíza Conselheira Helena Moniz[11].

Numa opção que que dificilmente se compreende tendo em conta a acrescida relevância ético-social dos dados pessoais e da sua proteção nos nossos dias – atestada pela própria aprovação do RGPD e pelo significativo aumento da recolha e tráfego de dados nas últimas duas décadas –, o legislador manteve as mesmas penas do crime previsto no artigo 43.º, da Lei n.º 67/98, de 26 de outubro, tanto para o tipo simples, como para o tipo agravado: respetivamente um ano de prisão ou cento e vinte dias de multa (*Cfr.* artigo 48.º, n.º 1, da LPD) e dois anos de prisão ou duzentos e quarenta dias de multa (*Cfr.* artigo 48.º, n.ºs 2 e 3, da LPD).

Nos termos do artigo 48.º, n.º 2, da LPD, as penas são agravadas para o dobro dos seus limites quando estiverem em causa as categorias especiais de dados previstas nos artigos 9.º e 10.º do RGPD e, nos termos das alíneas a) e b) do n.º 3 do mesmo artigo, quando o "acesso" for realizado *(i)* com violação de regras técnicas de segurança ou *(ii)* quando tiver proporcionado ao agente ou a terceiros benefício ou vantagem patrimonial. Todavia, adiantamos, desde já, que a punição pela prática do crime desvio de dados agravado nos termos do n.º 3 do artigo 48.º da LPD oferece as maiores dúvidas.

Em primeiro lugar, note-se que a punição agravada diz respeito, literalmente, ao "acesso" aos dados pessoais e não à cópia, à subtração, à cedência ou à transferência dos dados pessoais. Resulta assim evidente que o crime desvio de dados nesta modalidade agravada só poderia ser praticado quando, além das ações típicas descritas no n.º 1 do artigo 48.º da LPD, se tivesse verificado o acesso aos dados pessoais com violação de regras técnicas de segurança ou com benefício ou vantagem patrimonial para o próprio ou para terceiros. Dito de outra forma, o desvio de dados com violação de regras técnicas de segurança ou com benefício ou vantagem patrimonial não é objeto de agravação, o que se afigura incompreensível na economia do regime.

Em segundo lugar, a aplicar-se literalmente este tipo agravado, a punição do desvio de dados agravado conduziria a um problema de concurso de crimes. Em rigor, a conduta prevista no artigo 48.º, n.º 3, da LPD é já punida autonomamente pelo artigo 47.º, n.º 3, da LPD, pelo que, à luz dos princípios acima referidos, o agente que aceda a dados pessoais, com violação de regras técnicas de segurança ou com benefício ou vantagem própria para si ou para terceiros e que, posteriormente, copie, subtraia, ceda ou transfira dados pessoais sem previsão legal ou consentimento poderá ser punido por um crime de acesso indevido agravado, nos termos do artigo 47.º, n.ºs 1 e 3, da LPD e por um crime de desvio de dados simples, nos termos do artigo 48.º, n.º 1. Admitir outra solução, designadamente no sentido de acumular as modalidades agravadas dos crimes dos artigos 47.º, n.º 3, e 48.º, n.º 3, esbarraria no regime do concurso aparente e seria, ademais, desautorizada pelo princípio *non bis in idem*, inscrito no artigo 29.º, n.º 5, da Constituição, uma vez que essa hipótese implicaria valorar duas vezes, *e contra reo*, o acesso indevido realizado em violação de regras técnicas de segurança.

Já o agente que legitimamente aceder aos dados pessoais e que, posteriormente, copiar, subtrair, ceder ou transferir esses mesmos dados, ainda que esse desvio seja feito com violação de regras técnicas de segurança ou com benefício ou vantagem patrimonial para terceiros, apenas poderá ser punido pelo tipo simples do artigo 48.º, n.º 1, da LPD, e nunca pelo seu tipo agravado. Com respeito por opinião contrária[12],

termos do seu artigo 2.º, n.º 2, alínea c), o RGPD não se aplica quantos os dados pessoais sejam tratados para fins exclusivamente pessoais por parte de uma pessoa singular.

[10] Aqui no sentido comum e não na aceção do artigo 4.º, 10), do RGPD.

[11] Acessível em www.dgsi.pt.

[12] Pedro Venâncio, *ob. loc. cit.*, afirma que "*Quem, por qualquer meio, aceda a dados pessoais sem previsão ou*

a letra do artigo 48.º, n.º 3, não autoriza entendimento distinto, tanto mais quanto, no que respeita à alínea a), não se alcança sequer se, de facto, o legislador quis agravar as condutas que consubstanciam o desvio quando praticadas com violação de regras técnicas de segurança, ou se antes pretendeu agravar a prática do crime desvio de dados quando as condutas que consubstanciam o desvio foram precedidas do acesso aos dados pessoais com violação de regras técnicas de segurança. A primeira solução é de sustentação impossível, porquanto não encontra qualquer suporte no sentido possível das palavras utilizadas no n.º 3 do aludido artigo 48.º, que alude apenas a "*acesso*" e nunca a "*desvio*", sendo certo que é dentro da delimitação desse sentido possível das palavras que se funda a interpretação permitida em Direito Penal e a fronteira face à regra da proibição da analogia resultante do artigo 1.º, n.º 3, do Código Penal[13]. Já a segunda solução, suscita o problema de concurso já anteriormente apontado.

Aliás, a deficiência da redação daquela norma é de tal ordem que não permite ao intérprete descortinar, com o mínimo de segurança imposto pelo princípio da legalidade, se o legislador pretendeu agravar todas as modalidades típicas do crime ou apenas algumas delas. Do ponto de vista da ofensa do bem jurídico não será igual o agente simplesmente copiar dados ou transferir dados pessoais para terceiros.

3. O desvio de dados e as condições de licitude de tratamento de dados pessoais

Relativamente ao tipo (simples) do crime de desvio de dados importa densificar as dúvidas previamente enunciadas e que se reconduzem à questão de saber quando é que a cópia, a subtração, a cedência ou a transferência de dados pessoais preenchem o tipo do crime de desvio de dados.

O legislador do artigo 48.º da LPD optou por proteger a privacidade e a autodeterminação informacional mediante a proibição um conjunto de operações sobre dados pessoais quando estas sejam realizadas sem prévia *previsão legal* ou *consentimento*, mas, como se adiantou, não é evidente o que constitua "*previsão legal*".

Ora, constatando que as operações tipificadas na norma penal são formas de tratamento de dados pessoais, nos termos do artigo 4.º, 2), do RGPD, importa, antes de mais, deslindar quais são os requisitos a que esses tratamentos de dados estão sujeitos: quando é que as pessoas singulares e coletivas podem tratar dados pessoais (?).

Sem prejuízo naturalmente de outras obrigações a que os responsáveis pelos tratamentos de dados pessoais estão sujeitos, quanto ao crime do artigo 48.º da LPD – ao contrário do que sucede com o crime do artigo 46.º que convoca especialmente o princípio da finalidade (*Cfr.* artigo 5.º, n.º 1, alínea b), do RGPD) –, destaca-se, entre as normas aplicáveis, o princípio da licitude do tratamento de dados pessoais consagrado no artigo 5.º, n.º 1, al. a), do RGPD.

Em termos rigorosos, este princípio impõe que antes de realizar qualquer operação de tratamento de dados pessoais, os responsáveis terão de assegurar-se de que, pelo menos, uma entre as seis condições de licitude de tratamento de dados pessoais, previstas no artigo 6.º do RGPD, está verificada. Neste sentido, é o próprio legislador europeu que o esclarece no Considerando § 40 do RGPD: "*Para que o tratamento seja lícito, os dados pessoais deverão ser tratados com base no consentimento da titular dos dados em causa ou noutro fundamento legítimo, previsto por lei, quer no presente regulamento quer noutro ato de direito da União ou de um Estado-Membro referido no presente regulamento, incluindo a necessidade de serem cumpridas as obrigações legais a que o responsável pelo tratamento se encontre sujeito ou a necessidade de serem executados contratos em que o titular dos dados seja parte ou a fim de serem efetuadas as diligências pré-contratuais que o titular dos dados solicitar*".

Como ensina, António Barreto Menezes Cordeiro, "*Em sentido estrito, o princípio da licitude determina que todo e qualquer tratamento de dados pessoais encontre o seu fundamento numa norma permissiva*"[14].

Isto é, sempre que uma pessoa coletiva ou singular pretenda tratar dados pessoais – sempre na aceção ampla da norma do RGPD – terá previamente de verificar se está assegurada uma das seis condições licitude legalmente consagradas: *(i)* a existência de consentimento do titular dos dados para o seu tratamento (*Cfr.* artigo 6.º, n.º 1al. a), do RGPD); *(ii)* a necessidade de tratar os dados pessoais no que for estritamente necessário à celebração a seu pedido ou à execução de um contrato em que o titular seja parte (*Cfr.* artigo 6.º, n.º 1al. b), do RGPD); *(iii)* o tratamento é imprescindível para o cumprimento de uma obrigação

consentimento e os utilize («copiar, subtrair, ceder ou transferir») para um qualquer fim (igual ou diferente daquele que determinou a sua recolha comete o crime de desvio de dados".

[13] Sobre os limites à proibição da analogia e a delimitação da interpretação permitida em Direto Penal, entre outros, Jorge de Figueiredo Dias, *Direito Penal – Parte Geral: Tomo I: Questões fundamentais. A Doutrina Geral do Crime*, 3.ª Edição, Gestlegal, Coimbra, 2019, pp. 220-227; Maria Fernanda Palma, *Direito Penal – Conceito material de crime, princípios e fundamentos. Teoria da lei penal: interpretação, aplicação no tempo, no espaço e quanto às pessoas*, 4.ª edição, AAFDL Editora, Lisboa, 2019, pp. 140-157.

[14] In *Comentário ao Regulamento Geral de Proteção de dados*, cit., p.102.

legal (*Cfr.* artigo 6.º , n.º 1, al. c), do RGPD); *(iv)* o tratamento é necessário para assegurar um interesse vital do titular dos dados (*Cfr.* artigo 6.º , n.º 1, al. d), do RGPD); *(v)* o tratamento destina-se ao cumprimento de funções de interesse público do responsável (*Cfr.* artigo 6.º , n.º 1, al. e), do RGPD) e *(vi)* o tratamento sustenta-se na existência de um interesse legítimo prevalecente do responsável (*Cfr.* artigo 6.º, n.º 1, al. f), do RGPD). Acrescem, ainda, a estas condições de licitude as condições de licitude especiais do catálogo previsto no artigo 9.º do RGPD para o tratamento de categoriais especiais de dados.

Na verdade, a ideia de tratamento lícito enquanto tratamento sustentado num elenco fechado de casos legalmente pré-determinados[15], naquilo a que na terminologia da proteção de dados se tem denominado por *condições de licitude* ou *condições de legitimidade* ("legal basis" ou "grounds for processing" na língua inglesa), decorre outrossim quer do artigo 5.º, n.º 2, da Convenção 108 modernizada[16], quer do artigo 8.º, n.º 2, da Carta dos Direitos Fundamentais da União Europeia.

Se é verdade que a menos conseguida redação da norma do artigo 48.º, n.º 1, da LPD pode causar embaraços ao intérprete seja porque "previsão legal" não é um termo empregue no RGPD ou noutros instrumentos legais de proteção de dados, seja porque o termo parece conduzir o intérprete a normas legais que consagrem a possibilidade ou a obrigação de copiar, subtrair, ceder ou transferir dados pessoais[17], a verdade é que seria injustificado punir criminalmente condutas que, afinal, são permitidas por outras normas legais.

Com efeito, no plano do RGPD não há dúvidas de que operações como cópia, apagamento ou transferência de dados pessoais são operações típicas de tratamentos de dados pessoais. Sem prejuízo do cumprimento de outras normas que visam proteger os dados pessoais, *ab initio*, os tratamentos de dados pessoais, independentemente das concretas operações físicas ou digitais que sejam realizadas com os mesmos, apenas serão lícitos se estiver previamente verificada pelo menos uma das seis condições de licitude previstas no artigo 6.º do RGPD, pelo que a pessoa singular ou coletiva que pretenda copiar, subtrair, ceder ou transferir dados pessoais poderá fazê-lo licitamente se uma daquelas condições estiver prevista.

Estas conclusões permitiriam convocar o *tipo justificador*, seguindo a doutrina de Figueiredo Dias[18], consagrado no artigo 31.º, n.º 1, do CP, uma vez que, independentemente da posição que se tome sobre a *unidade integral da ilicitude jurídica*, não parecem existir dúvidas do que esclarece Paulo Pinto de Albuquerque "(...) *sendo a ação licita face a qualquer parte do ordenamento jurídico, também o é para o direito penal* (...)"[19]. Todavia, cremos que a nossa dúvida fundamental deve resolver-se ainda no anterior plano da tipicidade.

A redação da norma do artigo 48.º, n. 1, da LPD, é infeliz. Como se sublinhou, "previsão legal" não é um termo que se encontre no Código Penal, no RGPD ou noutras normas que visam a proteção de dados pessoais e poderia, à primeira vista, conduzir o intérprete a considerar que o crime do artigo 48.º, n.º 1, da LPD seria praticado sempre que inexistisse consentimento do titular ou normal legal específica que previsse a possibilidade ou a obrigação de copiar, subtrair, ceder ou transferir os dados pessoais ou, pelo menos, uma obrigação específica ainda que genérica de tratamento de dados.

Porém, a infelicidade do legislador não autoriza tais resultados hermenêuticos. Se é inquestionável, como verificámos, que existe um elenco taxativo de condições de licitude para o tratamento de dados pessoais, não pode ser desconsiderado, no plano da técnica legislativa, que o legislador tende a separar o consentimento e as demais condições de licitude.

No Considerando § 40 do RGPD pode ler-se "(...) *com base no consentimento da titular dos dados em causa ou noutro fundamento legítimo, previsto por lei* (...)"; no artigo 5.º, n.º 2, da Convenção 108 modernizada encontram-se "*Cada Parte deverá assegurar que o tratamento de dados possa ser efetuado com base no consentimento livre, específico, informado e inequívoco do titular dos dados ou em qualquer outro fundamento legítimo previsto na legislação*" e no artigo 8.º, nº 2, da Carta dos Direitos Fundamentais da União Europeia estabeleceu-se "*Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto na lei*".

---

[15] Sobre o elenco fechado de condições de licitude, mas a propósito a transferência de dados de um responsável para outro responsável pelo tratamento, *vide* Acórdão do Tribunal de Justiça da União Europeia, de 4 de Outubro de 2024, no processo C-621/22, *Koninklijke Nederlandse Lawn Tennisbond*.

[16] *Cfr. Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal*.

[17] Note-se que a condição de licitude prevista no artigo 6.º, n.º 1, al. c), do RGPD é amiúde designada por "obrigação legal". A título de exemplo, veja-se *Manual da Legislação Europeia da Proteção de Dados*, da Agência para os Direitos Fundamentais da União Europeia, p. 134, acessível em: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_pt.pdf.

[18] In *Direito Penal*, Tomo I, Coimbra Editora, 3.ª Ed, 2004, pp. 363 a 369.

[19] In *Comentário do Código Penal*, 3.ª Ed., UCE, 2015, p.226.

Pese embora, no plano da proteção de dados, não apoiemos a distinção da legitimidade dos tratamentos de dados pessoais realizados com base no consentimento da legitimidade dos tratamentos realizados com base noutras condições de licitude[20/21] – desde logo, porque a própria formulação do artigo 6.º do RGPD não o autoriza, mas também porque o consentimento nem sempre é uma condição de licitude adequada ao tratamento de dados concreto e nem sequer se pode afirmar que, em tempos hodiernos, o consentimento seja, por si só, o instrumento mais adequado à proteção dos dados pessoais –, é inegável, seja por tradição jurídica, seja por referência aos instrumentos internacionais e europeus da proteção de dados, que o legislador europeu se socorre recorrentemente da fórmula que separa consentimento de outros fundamentos legais ou legítimos.

Cremos que o nosso legislador, malgrado o resultado deficiente do seu labor, pretendeu simplesmente decalcar para a norma do artigo 48.º LPD essas fórmulas binómicas de outros normativos que consagram o princípio da licitude do tratamento dos dados pessoais, estabelecendo uma versão simplificada, ainda que pouco clara, daquelas.

Em qualquer caso, não hesitamos em afirmar que o tipo de crime de desvio de dados, consagrado no artigo 48.º, n.º 1 da LPD, deve ser interpretado da seguinte forma: "*Quem copiar, subtrair, ceder ou transferir, a título oneroso ou gratuito, dados pessoais sem consentimento* [ou outro fundamento legítimo previsto na lei], *independentemente da finalidade prosseguida, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias*".

4. O "consentimento" do artigo 48.º da LPD

Cremos que não valerá a pena alongarmo-nos também no que respeita ao segmento típico referente ao consentimento. Com efeito, ao nível da tipicidade parece-nos indiscutível que o consentimento do artigo 48.º será o consentimento previsto quer no artigo 6.º, n.º 1, alínea a), quer no artigo 9.º, n.º 2, alínea a), ambos do RGPD e com os requisitos de validade enunciados naquele Regulamento (*Cfr.* artigos 7.º e 4.º, 11)).

Na verdade, como se pretendeu demonstrar, o legislador da LPD procurou punir criminalmente quem sem reunir condição de licitude válida, por referência ao elenco de condições de licitude válidas dos artigos 6.º e 9.º do RGPD, *desvie*, respetivamente, dados pessoais e categorias especiais de dados. Não vermos, por isso, sentido em diferenciar os requisitos do consentimento das demais condições de licitude.

Todavia, tal não implica que, ao nível da ilicitude, não se possa considerar verificada uma causa de exclusão de ilicitude (*Cfr.* artigo 30, n.º 1 e n.º 2 al. d), do CP) sempre que se verifique um consentimento explícito ou presumido, nos termos e para os efeitos do disposto respetivamente nos artigos 38.º e 39.º do CP. A verificação destas causas legais de exclusão de ilicitude, baseando-se em fórmulas jurídicas de consentimento menos onerosas que as resultantes do RGPD, deve, ainda assim, valer, nos termos gerais, para que a conduta de desvio de dados se tenha como justificada – o que, gerando efeitos automáticos no afastamento da imputação criminal, já não terá relevância no que respeita ao quadro contraordenacional abstratamente aplicável perante um desvio de dados baseado numa declaração de consentimento aquém das exigências do RGPD.

[20] Neste sentido parece ir tanto a Opinião 5/2011, WP 187, do Grupo do Artigo 29.º, como as Orientações 5/2020 do Comité Europeu da Proteção de Dados.

[21] Em sentido parcialmente distinto, Christopher Kuner, *et al.*, *The EU General Data Protection Regulation (GDPR), A Commentary*, Oxford, 2020, p. 329: "*There is no ranking between Article 6(1)(a)-(f) in the sense that one ground has normative priority over the others. However, in the private sector, consent (Article 6(1)(a)) may in practice play a salient role as a potential substitute whenever there is no contractual context, no detailed legal rules about a fitting legal basis or the scope of "legitimate interests of the controller or of a third party" is particularly difficult to assess*".