O MODELO DE SUPERVISÃO DE TRATAMENTOS DE DADOS PESSOAIS NA UNIÃO EUROPEIA: DA ATUAL DIRETIVA AO FUTURO REGULAMENTO

Filipa Calvão*

*) Professora Auxiliar da Faculdade de Direito da Universidade Católica Portuguesa. Investigadora do *Católica Research Center for the Future of Law*. Presidente da Comissão Nacional de Protecção de Dados.

1. A SUPERVISÃO DOS TRATAMENTOS DE DADOS PESSOAIS NA UNIÃO EUROPEIA E EM PORTUGAL: REGIME ATUAL

A proteção de dados pessoais afirmou-se em Portugal e na Europa num período em que o modelo de regulação jurídica de atividades privadas, em diversas áreas, assentava em grande medida ainda no controlo administrativo prévio das mesmas para verificar se do seu desenvolvimento não resultava a violação de interesses públicos ou a violação insuportável dos direitos dos indivíduos. Esse modelo é acompanhado de outros poderes fundamentais: regulamentação, supervisão *ex post* (fiscalização) e sancionamento. No seu conjunto, estes poderes permitem às entidades administrativas reguladoras orientar as condutas dos regulados, de modo a prevenir ou corrigir comportamentos que ponham em causa os valores ou direitos que aquelas têm por função tutelar[1].

Foi esse modelo de supervisão *ex ante* e *ex post* que a Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados, assumiu em relação aos tratamentos de dados que apresentam maiores riscos para o direito à proteção de dados pessoais, e que, portanto, foi consagrado na generalidade dos diplomas legais que procederam à sua transposição para a ordem jurídica dos Estados membros da União Europeia – veja-se o artigo 20.º da Diretiva.

Nos restantes tratamentos de dados pessoais, dotados portanto de menor risco para os direitos e liberdades, a Diretiva traça o caminho preferencial do controlo *a posteriori* pela autoridade administrativa dos tratamentos de dados (v. considerando 52), apenas admitindo como regra a notificação prévia dos mesmos à autoridade administrativa de controlo, com o objetivo, assumido no considerando 48, de assegurar a publicidade das finalidades e principais características do tratamento – por forma a dar a conhecer quem, e em que termos, está no mercado a fazer tratamentos de dados.

1) No que às atividades públicas e privadas que envolvem tratamentos de dados pessoais diz respeito, a função de regulamentação é sobretudo concretizada através da emissão de orientações não vinculativas (e outros instrumentos jurídicos de *soft law*, como seja a aprovação de códigos de condutas ou manuais de boas práticas) dirigidas aos responsáveis pelos tratamentos de dados, as quais constituem simultaneamente uma referência/padrão para os titulares dos dados tratados.

Donde resulta que, quando uma pessoa singular ou uma pessoa coletiva pretenda iniciar uma atividade comercial, profissional, de investigação ou outra (independentemente da natureza privada ou pública do setor onde a mesma seja desenvolvida) que envolva tratamento de dados pessoais, teremos as mais das vezes um simples sistema de notificação para efeito de registo (aquilo que agora se usa chamar de comunicação prévia sem prazo), e em casos de maior risco, por incidir sobre dados pessoais sensíveis ou pelo contexto ou dimensão do tratamento, um sistema de controlo administrativo prévio, a realizar pela autoridade de controlo nacional – no caso português, a Comissão Nacional de Protecção de Dados – e que passa pela emissão (ou recusa de emissão) de uma autorização administrativa. Foi esta a solução acolhida entre nós, como o revelam os artigos 27.º e 28.º da Lei n.º 67/98, de 26 de outubro, que transpôs para a nossa ordem jurídica aquela Diretiva.

Quanto às situações de maior risco para a privacidade – e que correspondem, grosso modo, aos dados elencados no artigo 7.º e ainda no artigo 8.º da Lei n.º 67/98, de 26 de outubro – parte-se da proibição do tratamento dos mesmos, mas admitindo a lei que a proibição possa ser afastada mediante autorização (proibição com reserva de autorização[2]). Será no âmbito do procedimento autorizativo que se verificará o cumprimento dos requisitos que a lei define para o exercício da atividade – aqui o tratamento dos dados pessoais – como condição desse exercício, de modo que daí não resulte perigo ou risco para os direitos das pessoas. Precisamente por isso é comum encontrar-se nos atos autorizativos a imposição de condições e limites ao tratamento de dados pessoais, por só assim se poder eliminar ou reduzir a um mínimo, tido por indispensável e justificado, a afetação dos direitos que um tratamento de dados pessoais sempre implicará[3].

Certo é que o controlo administrativo prévio assim instituído visa verificar e garantir, através da imposição de limites e obrigações vários, que o tratamento não afeta o conteúdo essencial dos direitos à proteção de dados pessoais e à reserva da intimidade da vida privada, ou de outros direitos, liberdades e garantias que por via dele possam ser afetados, e que apenas os comprime na medida mínima indispensável à prossecução da finalidade legítima que com esse tratamento se visa alcançar.

Naturalmente que deste regime jurídico resultava – e resulta – um retardamento do início da atividade no âmbito da qual se quer realizar o tratamento de dados pessoais, com evidente prejuízo para os cidadãos, empresas ou instituições públicas requerentes e, consequentemente, para a economia, a investigação científica e demais interesses públicos em causa.

2) V. por todos, Pedro Costa Gonçalves, *Reflexões sobre o Estado Regulador e o Estado Contratante*, Direito Público e Regulação 8, Cedipre, Coimbra Editora, Coimbra 2013, pp. 146—148.

3) Note-se que, em rigor, este controlo prévio não se esgota na decisão autorizativa a emitir no âmbito de procedimentos administrativos concretos. A Diretiva, no n.º 3 do artigo 20.º, consagra ainda como forma de exercício do controlo prévio pela autoridade de controlo a possibilidade de os Estados membros preverem a intervenção da autoridade no âmbito dos procedimentos legislativos ou de criação de outras normas jurídicas que regulem tratamentos de dados pessoais, solução que foi acolhida no direito português (cf. n.º 2 do artigo 22.º e alínea a) do n.º 1 do artigo 23.º da Lei n.º 67/98, de 26 de outubro).

No plano europeu, a necessidade de operadores económicos solicitarem autorizações em cada Estado membro em cujo território pretendam estabelecer-se ou realizar operações sobre dados sensíveis acaba por representar um entrave à livre circulação de bens e serviços, de capitais, no fundo, um entrave à liberdade de estabelecimento e de prestação de serviços – princípios pilares da União Europeia[4]. Com a agravante de, como os regimes jurídicos de proteção de dados dos Estados membros não apresentam hoje exatamente os mesmos contornos, os dados pessoais receberem dentro do espaço europeu níveis de proteção não exatamente coincidentes[5]. Circunstância utilizada por alguns Estados como chamariz para o estabelecimento de grandes grupos económicos, com perturbação da concorrência no espaço europeu e em prejuízo da tutela dos direitos fundamentais dos seus cidadãos.

Compreenda-se, contudo, que tal prejuízo se apresentará como necessário para salvaguardar um direito fundamental que tão ameaçado é nos dias de hoje, em boa parte por causa da generalização do uso de tecnologias e sistemas de informação que implicam operações sobre informação pessoal[6].

Foram essencialmente estas considerações que levaram a Comissão Europeia a apresentar uma proposta de Regulamento que garantisse um regime harmonizado da proteção de dados pessoais no espaço económico europeu, e que refletisse aquela que é a orientação do Direito da União Europeia nos tempos mais recentes: a eliminação do controlo administrativo prévio, como forma de realizar plenamente o princípio da liberdade de circulação no espaço europeu[7]. Na verdade, na senda de jurisprudência do Tribunal de Justiça da União Europeia, a eliminação do controlo prévio foi assumida como objetivo, trave mestra, do mercado europeu, como meio de promover o direito de estabelecimento e a liberdade de prestação de serviços. Expressão inequívoca desta tendência é a Diretiva 2006/123/CE, de 12 de dezembro de 2006, relativa aos serviços no mercado interno, que veio proibir o regime de autorização, exceto nas condições descritas nos artigos 9.º e seguintes (onde se prevê a admissão condicionada do regime autorizativo).

4) E de, em abstrato, tais controlos prévios realizados no plano nacional pela correspondente autoridade de controlo, poderem, se previstos como momentos de exercício de um poder discricionário menos densificado por lei, importar o risco de servir políticas protecionistas dos operadores nacionais. É certo que a Diretiva procura prevenir este risco, reconhecendo que quem estiver autorizado a (ou, nos termos da lei nacional do Estado onde tem estabelecimento, em condições de) realizar um tratamento de dados pessoais no território desse Estado membro pode fazê-lo no território de outro Estado membro, ao abrigo da lei nacional do Estado de origem, sem necessidade de controlo prévio daquele.

5) Há quem, a este propósito, se refira a uma lacuna de regulação europeia ou supranacional, regulação essa que se concretiza no plano normativo, e que o Regulamento europeu pretende suprir – cf. Philip Schütz, «The Set Up of Data Protection Authorities as a New Regulatory Approach», in Serge Gutwirth/ Ronald Leenes / Paul de Hert / Yves Poullet (org.), *European Data Protection: in Good Health?,* Springer, 2012, pp. 125-142 (128).

6) Para uma descrição do impacto da utilização da tecnologia na privacidade, apresentada em 1995, ano da aprovação da Diretiva 95/46/CE, v. Pierre Kayser, *La protection de la vie privée par le Droit. Protection du secret de la vie privée*, 3.ª ed., Ed. Economica, 1995, pp. 206-220. Para desenvolvimentos mais recentes, em especial associados ao fenómeno do *Big Data* e do *data mining* e os correspondentes riscos de criação perfis, v. Viktor Mayer-Schönberger/ Kenneth Cukier, *Big Data. A Revolution that will Transform How we live, work and think,* John Murray, London, 2013, p. 150-171; Serge Gutwirth/ Mireille Hildebrandt, «Some Caveats on Profiling», in Serge Gutwirth/ Yves Poullet/ Paul De Hert, *Data Protection in a Profiled World*, Springer, 2010, pp. 31-41.

7) Falando de uma mudança na cultura administrativa, que se caracteriza pela passagem de uma Administração Pública legalmente orientada para uma Administração Pública economicamente orientada, Christoph Holtwisch, «Die Informationstechnologische Verwaltung im Kontext der Verwaltungsmoderniesierung – Bürger und Verwaltung in der Internet-Demokratie», in *Die Verwaltung* 2010 (Heft 4), pp. 567-591 (572).

A tendencial eliminação do sistema de controlo administrativo prévio, descentrando o controlo ou supervisão administrativa para um momento ulterior, de acompanhamento da atividade, não pode, todavia, ser feita sem mais. Se é verdade que se assiste hoje a uma crescente simplificação dos procedimentos de acesso ao mercado e de início de atividades, não é menos verdade que, como sublinha Pedro Gonçalves, «[…] a transformação operada neste domínio, do controlo do acesso ao mercado, está ainda longe de poder reconduzir-se à ideia simples de desregulação. Com efeito, há sintomas claros de uma transformação que aponta, isso sim, para uma maior exigência regulamentar à entrada no mercado e para o reforço da regulação pública *ex post*»[8].

No que aos tratamentos de dados pessoais diz respeito, a função do Estado não se pode reduzir simplesmente ao acompanhamento sucessivo das atividades privadas (ou públicas), quando das mesmas possa resultar a afetação de direitos, liberdade e garantias dos membros da comunidade estatal. Isto porque, ao contrário de outras atividades, que são livres (porventura só agora desreguladas), por o seu desenvolvimento não implicar risco ou ameaça de direitos e de interesses privados e públicos, as operações que incidam sobre dados pessoais, qualquer que seja a sua natureza, não são, não podem ser livres. Falamos de atividades que são suscetíveis de ter impacto na liberdade, na privacidade, na autodeterminação ou na identidade das pessoas. E um tal impacto e um tal risco de lesão de dimensões fundamentais da dignidade da pessoa humana não podem ser ignorados, muito menos incentivados. É esta a razão por que na União Europeia não se abandona a regulação pública dos tratamentos de dados pessoais, definindo-se no plano normativo condições ou requisitos para a sua realização. E por isso a passagem do foco da função administrativa para o controlo sucessivo não reflete uma conceção de que o tratamento de dados pessoais é livre, quanto ao *se* da sua realização, e que o controlo se limite apenas ao *como* da atividade[9].

Assim, qualquer responsável por um tratamento de dados pessoais só poderá realizá-lo se cumprir os correspondentes pressupostos definidos no respetivo quadro regulamentar. Ora, é neste plano, da verificação prévia do preenchimento dos pressupostos legais, que se reflete a tendência moderna acima identificada.

O que se pretende agora é que o Estado, por intermédio da autoridade administrativa de controlo, abandone esta função verificativa e a transfira para os particulares – sejam eles os próprios operadores económicos, sejam eles terceiros. No primeiro caso, em que a tarefa de verificação do cumprimento de todos os pressupostos legais caiba aos interessados na realização do tratamento de dados, assistimos a um fenómeno de autorresponsabilização; no segundo caso, a ideia é a de transferir a competência verificativa para empresas ou profissionais a quem os Estados reconhecerão o poder de proceder a esse controlo (de certificação) [10].

8) *Op. cit.,* p. 144.

9) Cf. Pedro Gonçalves, *op. cit.,* p. 159, destacando que a perspetiva europeia em relação às atividades de prestação de serviços é a de que o controlo administrativo se restrinja ao *como* da atividade não quanto ao *se* da sua realização.

10) Sobre o tema, v. Pedro Gonçalves, *op. cit.,* pp. 150 e ss., máxime 160-162, que fala a este propósito na substituição do tradicional princípio da autoridade pública por um princípio de autorresponsabilização dos particulares.

O fenómeno, já identificado noutras áreas de atividade, de transferência da responsabilidade do controlo prévio para os privados facilita o início do exercício de atividades que envolvem tratamentos de dados pessoais e, com isso, garante a liberdade de circulação dos dados pessoais, tida desde cedo como essencial à concretização dos direitos ao estabelecimento e à livre prestação de serviços, que estiveram na base da regulação europeia vertida na Diretiva [11].

Tudo isto num momento em que se reconhecem as falhas na regulação (europeia e nacional) dos tratamentos de dados pessoais, muito por conta do elevado ritmo da evolução tecnológica e da perceção, frequentemente tardia, das consequências sobre a privacidade das renovadas utilizações dessa tecnologia, bem como do carácter transnacional e global dos tratamentos de dados pessoais (em boa medida imputável à Internet)[12].

Vejamos, sumariamente, em que termos se procura instituir este modelo na proposta de Regulamento.

2. O MODELO DE SUPERVISÃO DOS TRATAMENTOS DE DADOS PESSOAIS EM PROJETO

Como se referiu, está em curso o processo de discussão e aprovação de uma proposta de regulamento, apresentada pela Comissão Europeia, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados, doravante designada por Proposta de Regulamento)[13].

O objetivo assumido de «*assegurar um nível de proteção coerente e elevado das pessoas singulares e eliminar os obstáculos à circulação de dados pessoais, [que implica que] o nível de proteção dos direitos e liberdades das pessoas singulares relativamente ao tratamento desses dados deve ser equivalente em todos os Estados membros*» (cf. considerando 8), está na base da definição, por via de regulamento, de um regime harmonizado da proteção de dados pessoais no espaço económico europeu[14].

11) Sem pretender aqui discutir esta questão, que obrigaria a um parêntesis demasiado extenso, sempre se notará que a liberdade de circulação de dados pessoais não significa uma liberdade de tratamento dos mesmos: o ordenamento jurídico fixa, e deve fixar, limites, desde logo, quanto à recolha desses dados. Há de, pois, ser num quadro previamente regulamentado e limitado que os dados poderão circular.

12) Cf. Schütz, *op. cit.,* pp. 127-128.

13) Proposta de Regulamento de 25.01.2012 COM(1012) 11 final, disponível em http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_pt.pdf
Note-se que, embora a proposta neste momento em discussão e votação tenha já sofrido várias alterações, sobretudo promovidas pelo Parlamento Europeu, o documento que serve de base a esta apreciação corresponde à versão de 2012, a única que se encontra formalmente publicada.
Importa também observar que o pacote legislativo em discussão abarca ainda a proposta de diretiva para a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais, e à livre circulação desses dados, de 27.01.2012.

14) Sublinhando que a reduzida densidade ou precisão normativa da Proposta pode fazer fracassar o objetivo de harmonização, Peter Blume, «The myths pertaining to the proposed General Data Protection Regulation», in *International Data Privacy Law* (2014) 4, pp. 269-273, disponível em http://idpl.oxfordjournals.org/content/4/4/269.full

No que mais diretamente interessa ao tema aqui em análise, da leitura da Proposta de Regulamento ressalta a eliminação da supervisão prévia, com duas exceções. Quanto ao mais, os responsáveis por tratamento de dados pessoais realizam as operações sem ter de notificar o tratamento à autoridade administrativa de controlo – portanto, um regime de mera comunicação prévia, que não traduz um controlo prévio nem afeta o início do tratamento de dados[15], não mereceu acolhimento no Regulamento.

O controlo administrativo prévio, no tradicional modelo autorizativo, está previsto unicamente para as situações de transferências de dados pessoais para países terceiros ou para organizações internacionais, e a título excecional: apenas nos casos em que a Comissão Europeia não tenha tomado decisão de reconhecimento de um nível adequado de proteção de dados no Estado ou organização de destino e o responsável pelo tratamento ou um «subcontratante»[16] não tiverem apresentado garantias adequadas quanto à proteção dos dados num instrumento juridicamente vinculativo, nos termos definidos no n.º 5 do artigo 42.º da Proposta de Regulamento, ou adotem cláusulas contratuais que não correspondam às cláusulas-tipo a que se referem as alíneas *b)* e *c)* do n.º 2 desse mesmo artigo – cf. artigo 34.º, n.º 1, da Proposta de Regulamento.

A ideia é, pois, a de que o controlo público prévio é de afastar salvo se o controlo público sucessivo não for suficiente – ideia que não é nova, encontrando-se já refletida na Diretiva 95/46/CE (v. considerando 52 da Diretiva). Inequivocamente este é um dos casos em que o controlo prévio se justifica, não pelo facto de o controlo sucessivo não ser suficiente, mas por o mesmo ser impossível – não pode existir fiscalização *ex post* por parte das autoridades de controlo dos Estados membros da União sobre tratamentos dos dados transferidos que tenham lugar no território de Estados terceiros e de organizações internacionais.

Todavia, importa assinalar que o controlo administrativo sucessivo pode não ser suficiente em muitas outras situações, sobretudo quando se esteja perante informação pessoal mais sensível. É que o dano na privacidade (e nalguns casos na liberdade, que fica fortemente condicionada ou mesmo restringida por força da perda de privacidade) não é reintegrável – uma vez exposta ou devassada a vida privada, não é possível recuperar a privacidade que assim é atingida.

Talvez por essa razão, a Proposta de Regulamento, no n.º 2 do artigo 34.º, prevê um sistema de consulta prévia à autoridade de controlo, em dois tipos de hipóteses que

15) Sobre a mera comunicação prévia ou comunicação prévia sem prazo, v. Pedro Gonçalves, *op. cit.,* pp. 163-165; João Miranda, «A comunicação prévia no novo Código do Procedimento Administrativo», *in* Carla Amado Gomes/Ana Fernanda Neves/Tiago Serrão (coord.), *Comentários ao Novo Código do Procedimento Administrativo*, Lisboa, Associação Académica da Faculdade de Direito de Lisboa, 2015, pp. 495-511.

16) Aproveita-se a ocasião para notar que já vai sendo tempo de a tradução da expressão inglesa *processor* ou, na versão francesa, *sous-traitant* ser corrigida nos documentos da União Europeia: claramente a expressão «subcontratante» não corresponde ao conceito pretendido – quem subcontrata é o responsável, não (pelo menos, não necessariamente, já que em abstrato podem ocorrer vários níveis de subcontratação do processamento dos dados) aquele que vai processar os dados pessoais –, devendo, por isso, o mesmo ser substituído, à falta de melhor expressão, pelo termo *subcontratado*.

revelam específicos riscos para os direitos e liberdades dos titulares dos dados pessoais, em virtude da natureza, do âmbito ou da finalidade do tratamento de dados. Essas situações vêm identificadas, em termos abstratos, no n.º 2 do artigo 33.º[17], recaindo sobre a autoridade administrativa de controlo a tarefa de elaborar e publicitar uma lista das operações de tratamento que, na sua perspetiva, são suscetíveis de apresentar riscos específicos para os direitos e liberdades e, nessa medida, estão sujeitos a consulta prévia.

Nos termos definidos no n.º 3 do artigo 34.º, o procedimento de consulta apenas culmina com uma decisão da autoridade no caso de a mesma entender que o tratamento não cumpre o disposto no regulamento. Nesta hipótese, determina o mesmo preceito, a autoridade de controlo «proíbe o tratamento previsto e apresenta propostas adequadas para remediar essa falta de conformidade». Na verdade, este procedimento parece ter ainda em vista um tipo de controlo prévio que permita à autoridade administrativa opor-se ou proibir o tratamento de dados nos termos projetados, no contexto do qual o seu silêncio corresponderá a um "nada a opor" e um juízo negativo implica necessariamente a emissão de um ato administrativo proibitivo. Estaremos, pois, perante um procedimento de comunicação prévia (ou comunicação prévia com prazo)[18], que, ao contrário da mera comunicação, pressupõe a apreciação da legitimidade e dos termos do tratamento pela autoridade antes do início do tratamento – ao qual, aliás, o novo Código do Procedimento Administrativo faz referência no n.º 2 e n.º 3 do artigo 134.º. A esta função administrativa de controlo prévio soma-se um papel de orientação dos comportamentos ou operações de tratamento de dados – com a imposição do poder-dever de definir soluções em alternativa à originariamente projetada, a título de recomendação ou sugestão.

Duas notas merece ainda o artigo 34.º na parte respeitante à consulta prévia. A consulta prévia deve, nos termos definidos no seu n.º 2, ter lugar não apenas nos casos em que a autoridade entenda ser a mesma necessária (alínea *b)* do n.º 2 do artigo 34.º), como também nos casos em que «uma avaliação de impacto sobre a proteção de dados, como prevista no artigo 33.º, indicar que as operações de tratamento, devido à sua natureza, âmbito ou finalidade, podem apresentar um elevado nível de riscos específicos» (cf. alínea *a)* do n.º 2 do artigo 34.º) Todavia, parece haver aqui alguma tautologia. Com efeito, se a avaliação do impacto sobre a proteção de dados pessoais tem de ser feita sempre que as operações de tratamento apresentem riscos específicos para os direitos dos titulares dos dados (cf. n.º 1 do artigo 33.º), e se tal se tem por verificado – em especial – nas hipóteses descritas no n.º 2 do artigo 33.º, e se, por outro lado, a autoridade administrativa tem de publicitar uma lista de operações de tratamento suscetíveis de apresentar riscos específicos para os direitos dos titulares dos dados, pouco sobrará de efeito útil para a alínea *a)* do n.º 2 do artigo 34.º.

17) Reconduzindo-se, grosso modo, a tratamentos que visem a criação de perfis, que incidam sobre dados sensíveis, ou dados de crianças ou biométricos (nestas últimas hipóteses, apenas se no contexto de sistemas de arquivo de grande dimensão), pu que impliquem controlo por via de videovigilância ou por recurso a tecnologias similares.

18) Pedro Gonçalves, *op. cit.*, pp. 173-176. João Miranda, op. cit., pp. 499-502 (v. ainda pp. 504-507, onde o Autor alerta especificamente para as consequências deste controlo prévio no plano do controlo sucessivo).

A única forma de reconhecer a este preceito alguma autonomia ou efeito útil é interpretar o disposto no n.º 4 e na alínea *b)* do n.º 2 do artigo 34.º no sentido de o elenco de operações de tratamento de dados a elaborar pela autoridade administrativa incidir sobre operações não abarcadas pelo n.º 2 do artigo 33.º. Esta interpretação suporta-se ainda na referência a "em especial" contida no artigo 33.º, n.º 2, que aponta no sentido de que que se poderá justificar a realização de avaliação de impacto noutros casos. Assim, o dever de consulta prévia verifica-se sempre que o resultado da avaliação do impacto sobre a privacidade revelar elevado grau de riscos específicos, quanto a operações elencadas no n.º 2 do artigo 33.º; e sempre que as operações, não reconduzíveis às do elenco do n.º 2 do artigo 33.º, estejam sujeitas a consulta prévia por determinação da autoridade administrativa.

A segunda nota reporta-se ao n.º 4 do artigo 34.º. Na verdade, não se alcança como pode a autoridade de controlo comunicar a lista aos responsáveis pelo tratamento, se a lista deve ser feita em abstrato e a autoridade não conhece de antemão quem pretende realizar tratamentos de dados pessoais, já que não se consagra na Proposta de Regulamento o sistema de comunicação prévia dos tratamentos de dados.

Para além da imposição da realização de estudos ou avaliações do impacto sobre a proteção de dados pessoais, a Proposta de Regulamento institui ainda outras medidas que concretizam a intenção de mitigar os efeitos da falta de controlo administrativo prévio, transferindo a responsabilidade de garantia do cumprimento das regras e princípios de proteção de dados para o próprio interessado ou responsável, *i.e.,* aquele que realiza o tratamento de dados.

As mesmas vêm enunciadas no artigo 22.º, destacando-se, desde logo, o dever de designar um delegado para a proteção de dados.

A figura do *delegado para a proteção de dados* encontra-se regulada nos artigos 35.º a 37.º da Proposta de Regulamento. Esta é uma figura que já estava prevista como possível na Diretiva (cf. n.º 2 do artigo 18.º), mas que agora vem fixada a título imperativo, ainda que as situações em que a sua designação é obrigatória estejam delimitadas em função da natureza pública da entidade que realiza o tratamento, da dimensão da entidade privada responsável ou ainda das características do tratamento de dados pessoais realizado e do seu impacto sobre os titulares dos dados[19].

O delegado assume em boa medida as funções de controlo prévio e sucessivo que tradicionalmente eram da competência da autoridade administrativa (cf. artigo 37.º), constituindo a obrigação legal da sua criação uma expressiva manifestação da transferência do poder de controlo da autoridade administrativa para o próprio responsável pelo tratamento, que, noutros planos, tem vindo a ser institucionalizado (como sucede no domínio do direito do ambiente).

19) A solução de limitar este dever às entidades com um número determinado de trabalhadores (250 ou mais) tem sido objeto de fortes críticas na comunidade de proteção de dados pessoais. Ainda que se reconheça ser este um critério comum na definição normativa de obrigações das empresas, a verdade é que a dimensão da empresa não está numa relação direta e necessária (nem sequer tendencial) com o impacto dos tratamentos de dados por elas realizados sobre a privacidade das pessoas e sobre os seus dados pessoais.

Um outro dever vem imposto no artigo 22.º e desenvolvido nos artigos 31.º e 32.º da Proposta de Regulamento: o da notificação da violação de dados pessoais. Conhecido pela expressão abreviada, em língua inglesa, *Data Breach*, este dever de notificação foi inicialmente previsto na Diretiva relativa ao tratamento de dados pessoais e à proteção da privacidade nas comunicações eletrónicas (Diretiva e-Privacidade)[20].

Trata-se do dever que recai sobre o responsável de comunicar à autoridade administrativa de controlo o incumprimento das normas jurídicas de proteção de dados que possam afetar os direitos dos cidadãos, com indicação, entre outros elementos, das medidas adotadas ou propostas para remediar a violação dos dados pessoais – por forma a assegurar a fiscalização (*ex post*) da autoridade administrativa. A comunicação não é apenas dirigida à autoridade, mas também aos titulares dos dados, embora neste último caso apenas se a violação for suscetível de afetar negativamente a proteção dos dados pessoais ou a privacidade do seu titular.

O que se pretende agora, com a Proposta de Regulamento, é generalizar esta obrigação aos tratamentos de dados realizados em todos os setores de atividade. Naturalmente, a previsão deste dever pressupõe poderes efetivos da autoridade administrativa aptos a garantir a tutela dos direitos, desde logo quando o responsável não alerte a autoridade para a situação de violação. O que implica, à partida, o reconhecimento de poderes de inspeção e de sancionamento em caso de se verificar o incumprimento do dever de notificação[21].

Finalmente, destaca-se a obrigatoriedade de encontrar soluções tecnológicas que, logo na sua conceção ou "por defeito", assegurem uma menor intrusão na privacidade dos indivíduos (*Privacy Enhancing Technologies*) – cf. artigo 23.º da Proposta[22].

Embora se prevejam ainda outras formas de intervenção prévia, como seja a de aprovação de códigos de conduta ou de criação de mecanismos de certificação em matéria de proteção de dados e de selos e marcas de proteção de dados, a verdade é que, mais uma vez, essa função estará pensada para ser desempenhada pelos privados, reservando-se à autoridade administrativa o papel de promotor da elaboração ou criação destes instrumentos (cf. artigos 38.º e 39.º). O sistema está, pois, construído segundo

20) Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, alterada pela Diretiva 2009/136/CE, do Parlamento Europeu e do Conselho, de 25 de novembro.
Sobre o tema, v. o Parecer n.º 3/2014 do Grupo de Trabalho de Proteção de Dados (Grupo de Trabalho do Artigo 29.º), de 29.03.2014, disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

21) Neste sentido, Rosa Barcelo/ Peter Traung, «The Emerging European Union Security Brach Legal Framework: the 2002/58 ePrivacy Directive and Beyond», in Serge Gutwirth/ Yves Poullet/ Paul De Hert, *Data Protection in a Profiled World*, Springer, 2010, pp. 77-104 (p. 98).

22) E que se traduzem num conjunto de soluções tecnológicas que protegem a privacidade ao eliminar ou reduzir os dados pessoais tratados ou prevenindo o tratamento de dados pessoais que seja desnecessário ou indesejável, sem com isso perturbar a finalidade do tratamento dos dados. Tais soluções podem ser adotadas de raiz, aquando da conceção do sistema em que assenta o tratamento de dados pessoais (*Privacy by Design)* ou ter lugar como solução supletiva (*Privacy by Default).* Sobre o tema, em especial sobre as dificuldades de adoção destes sistemas, pode ver-se John J. Borking, «Why Adopting Privacy Technologies (PETs) Takes so Much Time», in Serge Gutwirth/ Yves Poullet / Paul de Hert / Ronald Leenes (org.), *Computers, Privacy and Data Protection: an Element of Choice,* Springer, 2011, pp. 309-341.

uma lógica de, passe a repetição, responsabilização (*accountability*) dos responsáveis pelos tratamentos de dados e de alívio da tarefa administrativa de controlo.

A eliminação, como regra, da supervisão prévia implica a concentração da intervenção administrativa no plano da orientação das condutas (recomendações, orientações gerais), e sobretudo no plano sucessivo, da fiscalização dos tratamentos de dados. Neste sentido, são atribuídos à autoridade administrativa de controlo os poderes de fiscalizar, de proibir tratamentos de dados e de sancionar. Tais poderes, elencados no artigo 53.º da Proposta de Regulamento, serão pois titulados por todas as autoridades administrativas de controlo nacionais, assim se corrigindo o desequilíbrio, que até agora se tem verificado entre os diferentes Estados membros, quanto à capacidade efetiva de intervenção administrativa para garantir os direitos dos cidadãos no contexto de tratamentos de dados pessoais. No caso português, daqui não decorrerá um incremento dessa capacidade, porque a Lei n.º 67/98, de 26 de outubro, assegura amplos poderes de investigação e de autoridade (cf. artigos 22.º, n.ºs 3 a 5, e 23.º, n.ºs 1 e 3).

Ainda no plano que nos ocupa, da supervisão, a Proposta de Regulamento introduz um novo mecanismo, vulgarmente denominado *one-stop-shop*, e que coloca novos problemas na proteção dos direitos e liberdades das pessoas singulares. Refiro-me ao modelo de simplificação administrativa do balcão único europeu, que implica existir apenas um interlocutor administrativo no espaço europeu em face de cada empresa – assente no critério do estabelecimento principal, o qual todavia não se encontra densificado na proposta.

Esta opção, que é acompanhada por um mecanismo de controlo de coerência – entre as autoridades de controlo dos Estados membros da União Europeia onde a empresa realiza operações sobre dados pessoais (cf. artigos 57.º e ss.) –, tem sido objeto de acesa discussão[23]. E as diferentes soluções entretanto propostas não resolvem de modo plenamente satisfatório a consequência principal, na perspetiva dos titulares dos dados, que é a do enfraquecimento da posição jurídica do cidadão na relação com o responsável do tratamento de dados. Com efeito, os mecanismos de controlo de coerência previstos na proposta de Regulamento não são suficientes para garantir a efetiva proteção do cidadão, parecendo antes conduzir-nos para uma Europa cada vez mais desigual: grupos económicos de grande dimensão *vs.* o cidadão isolado, apenas apoiado pela sua respetiva (porventura pequena) autoridade administrativa de controlo, contra quem, com grande probabilidade, se voltará um dia acusando-a de não lhe garantir uma proteção adequada.

A que se soma a desigualdade da posição jurídica (relativa) dos cidadãos europeus: será mais fácil o exercício dos direitos pelo titular dos dados tratados que se encontra no território do Estado membro onde está o estabelecimento principal da empresa, por comparação com a posição em que se encontra aquele que está no território de um Estado membro cuja autoridade administrativa não é a líder do procedimento de controlo dos tratamentos de dados.

23) V. o Parecer n.º 1/2012 do Grupo de Trabalho do Artigo 29.º, de 23.03.2012, em especial, pp. 18-21, disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf

3. CONCLUSÕES

Se a alteração do modelo de supervisão se pode entender como forma de corrigir muitas das desvantagens que o regime jurídico de supervisão prévia ainda vigente importa para a economia e para as empresas e outros organismos que realizam tratamentos de dados pessoais, agilizando ou acelerando a satisfação das finalidades que com os tratamentos de dados se tem em vista alcançar, também é evidente que esta reforma do regime de proteção de dados pessoais altera substancialmente a função das autoridades de controlo, destinando-lhes agora uma função mais reativa do que preventiva na tutela do direito à proteção de dados pessoais[24]. É certo que a tutela preventiva não desaparece completamente da missão das autoridades administrativas de controlo: como foi referido, reserva-se ainda uma função de orientação dos responsáveis quanto às condições e termos do tratamento de dados; nessa vertente, por via de orientações gerais ou recomendações individuais, as autoridades administrativas garantirão, com alguma eficácia, o cumprimento das regras e princípios da proteção de dados.

Note-se, contudo, que a transferência para os responsáveis pelos tratamentos dos dados da responsabilidade pelo cumprimento das condições e limites estabelecidos pelo regulamento (autorresponsabilização), nos termos acima explicados, e a canalização dos recursos públicos para a tarefa de controlo sucessivo, não é, *per se*, garantia de uma tutela eficaz dos direitos fundamentais no âmbito de tratamentos de dados pessoais.

Por um lado, a dimensão e extensão da transferência da responsabilidade para os responsáveis pelos tratamentos de dados pode levar a que a atividade administrativa se concretize, na prática, somente numa tarefa de «controlo do controlo»[25], ou seja, limitando-se à fiscalização dos processos internos de controlo realizados pelo próprio responsável do tratamento de dados, atuando apenas quando este, em cumprimento das obrigações normativas, notifica a autoridade administrativa da violação de dados pessoais.

Por outro lado, a autoridade administrativa não tem, nos termos definidos na Proposta de Regulamento, conhecimento de quem está a realizar tratamentos dados pessoais. Na verdade, com exceção dos casos em que os tratamentos dependem de autorização prévia ou em que tem de haver consulta prévia, a autoridade não é informada pelos responsáveis de que se iniciou o tratamento de dados. O que, em

24) Convém notar que a apreciação desta reforma está condicionada pelo facto de a proposta se ter abstido de densificar os mecanismos jurídicos que prevê, remetendo muitos dos aspetos essenciais do regime para atos delegados da Comissão Europeia, numa redistribuição de papéis normativos que parece contradizer o Tratado sobre o Funcionamento da União Europeia (cf. artigo 290.º). Sobre alguns aspetos de regime que mereceriam ser objeto de normação no próprio regulamento e não ser remetidos para atos delegados, pode ver-se o Parecer n.º 8/2012 do Grupo de Trabalho do Artigo 29.º, de 5.10.2012, disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp199_en.pdf

25) A expressão é empregada por Pedro Gonçalves mas com um sentido ou num contexto diferente – de controlo das entidades privadas que foram objeto de acreditação para realizar a certificação e de (hetero)controlo da atividade – cf. *op. cit.*, p. 162.

termos práticos, pode conduzir a que a supervisão sucessiva se limite às situações em que há queixas ou denúncias de tratamentos ilícitos, notificação da violação dos dados pessoais ou se restrinja aos organismos públicos e às empresas de maior dimensão, em relação aos quais é relativamente notório ou do conhecimento comum que certos tratamentos são realizados.

Ora, sempre se dirá que a opção pela eliminação do controlo administrativo prévio não implica necessariamente a dispensa de comunicação prévia dos tratamentos de dados pessoais (a realizar em termos simplificados, por exemplo, apenas para o simples efeito de identificação do tipo de tratamento e do respetivo responsável). Na verdade, esse seria um instrumento de grande utilidade para a autoridade de controlo conhecer quem está a realizar tratamentos de dados e as pessoas terem a perceção de que o seus dados estão a ser tratados e por quem. E essa é uma medida que noutros domínios de atividade o Direito da União Europeia tem admitido, precisamente porque permite o conhecimento do "mercado" (quem está a fazer o quê) e tem a vantagem de não bloquear ou retardar o início da atividade.

Finalmente, não pode deixar de se assinalar que a perspetiva adotada na Proposta de Regulamento, quanto à institucionalização ou não de supervisão administrativa prévia, assenta numa lógica de justificar o controlo nos casos em que seja de esperar um maior risco para os direitos e liberdades decorrente dos tratamentos de dados pessoais. Importa, porém, não esquecer que uma tal perspetiva não pretende apagar ou enfraquecer a proteção dos dados pessoais nos restantes casos. Na verdade, todos os dados pessoais merecem proteção na ordem jurídica europeia (como resulta do artigo 8.º da Carta dos Direitos Fundamentais da União Europeia), pelo que os responsáveis pelos tratamentos de dados pessoais, qualquer que seja o nível de risco deles decorrentes, sempre terão de observar os princípios e regras de proteção legalmente consagrados[26].

26) Neste sentido, veja-se a posição do Grupo de Trabalho do Artigo 29.º, vertida na declaração proferida a 30 de maio de 2014 – *Statement on the role of a risk-based approach in data protection legal frameworks* – disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf