FORUM
DE PROTEÇÃO DE DADOS

N.º 01 JULHO 2015 **SEMESTRAL**

EM FOCO

O NOVO QUADRO LEGAL EUROPEU

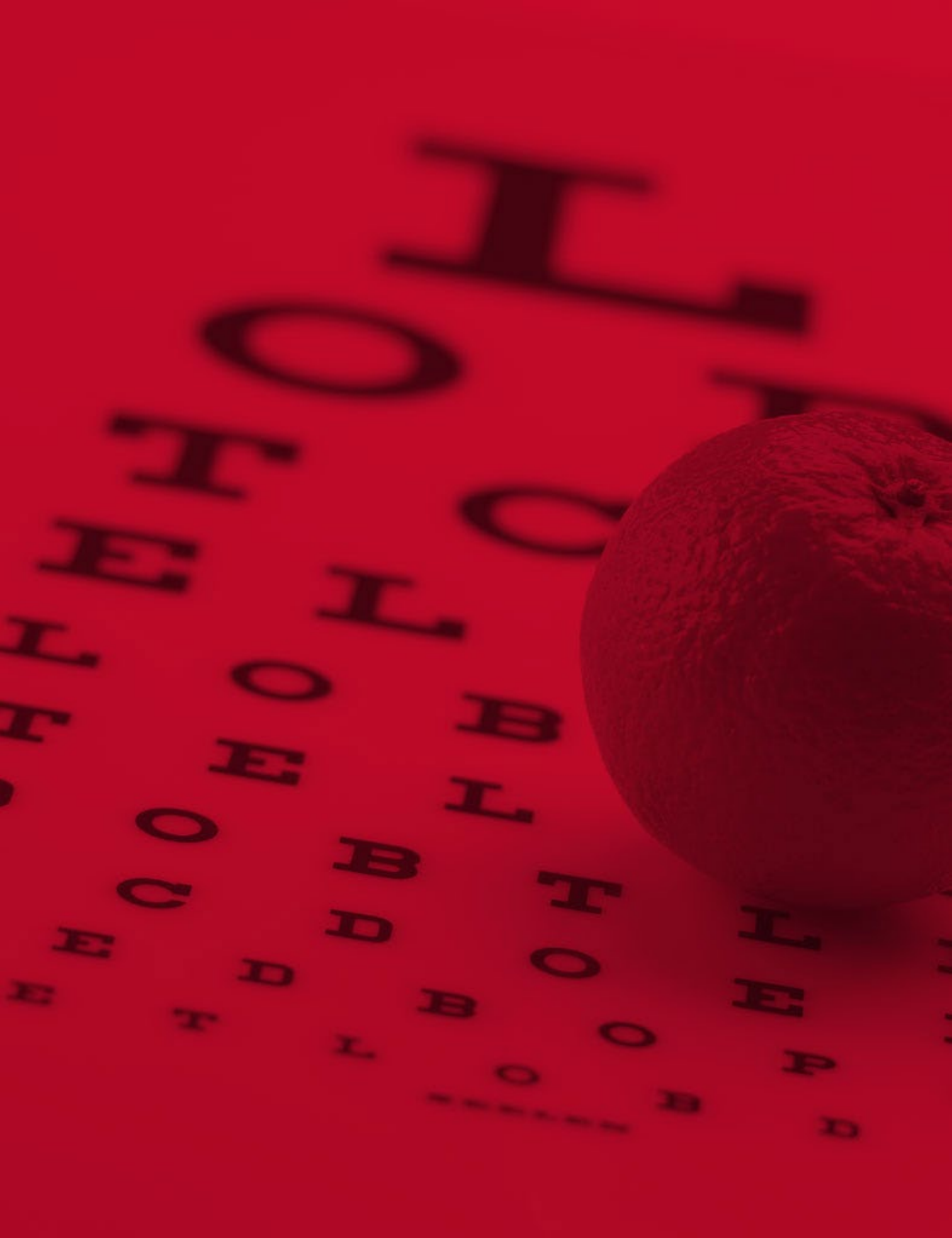
OPINIÃO DE JOSÉ VITOR MALHEIROS

TJUE - RETENÇÃO DE DADOS

DEVICE FINGERPRINTING

FORUM
DE PROTEÇÃO DE DADOS

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS



EDITORIAL

Volvidos pouco mais de vinte anos de intensa atividade em prol da defesa de direitos fundamentais dos cidadãos, a Comissão Nacional de Protecção de Dados (CNPD) entendeu ser tempo de alargar horizontes e empreender uma viagem em busca de abordagens atuais, de opiniões ousadas e de enfoques inovadores, reforçando assim a sua missão de promoção, difusão e esclarecimento das matérias de proteção de dados pessoais.

Fazia falta, no nosso país, um espaço de investigação, debate, opinião e divulgação sobre as questões da privacidade que nunca, como hoje, desempenharam um papel tão central e relevante na vida das pessoas e das sociedades. E assim nasceu o projeto desta revista, com uma prudente periodicidade semestral, mas com o objetivo de contribuir vigorosamente para a criação de um espaço aberto, plural e dinâmico.

Queremos fomentar a reflexão, incentivar o debate e promover a participação de todos. Privilegiamos a atualidade e a diversidade das áreas científicas, designadamente ciências sociais e ciências tecnológicas. Propomos que esta publicação seja um verdadeiro *forum* em torno dos assuntos de proteção de dados e da privacidade, transversal e abrangente.

O Forum de Proteção de Dados apresenta-se com secções regulares, embora flexíveis, colocando *Em Foco* textos de cariz científico ou centrados em questões delimitadas, destacando a *Jurisprudência* nacional e europeia mais relevante nesta área – sempre acompanhada de uma pequena anotação –, publicando *Documentos* oficiais (*v.g.*, pareceres, declarações) que merecem específica divulgação ou, ainda, contemplando rubricas dinâmicas, em função da atualidade, como o espaço de *Opinião* ou o espaço de *Debate*, pensados para acolher a perspetiva de uma ou várias personalidades da sociedade portuguesa sobre questões relacionadas com a privacidade.

Sendo por defeito um lugar de liberdade, as opiniões expressas não espelham necessariamente a posição oficial da CNPD, mesmo quando os artigos sejam da autoria de pessoas em relação direta com o organismo.

Estão lançados os dados para a promoção do pensamento e discussão sobre as novas ou renovadas questões que os tratamentos de dados pessoais e as recentes tendências de utilização das tecnologias suscitam.

Esperamos que embarquem nesta viagem connosco, pois estamos convictos do rumo que cursamos, a olhar para o futuro, mas sempre com os pés no presente.

Filipa Calvão

OPINIÃO

UM MUNDO
DE COISAS A ESCONDER

José Vítor Malheiros

"Se quiserem vasculhar a minha vida que vasculhem! Não tenho nada a esconder!"

É um argumento que ouvimos muitas vezes, em tom displicente, às vezes dito com orgulho ou mesmo em modo de desafio. No entanto, penso que é uma das posições mais lesivas da liberdade pessoal que existe nas nossas sociedades modernas, crescentemente vigiadas.

É um argumento que fragiliza mais ainda os mais fracos (os vigiados ou potencialmente vigiados), que reforça mais os poderes dos mais fortes (os que vigiam ou que podem vigiar) porque lhes garante total liberdade de acção, que apresenta como alienável um direito que é de facto inalienável, que compromete mais o nosso futuro, que põe em causa o nosso direito a viver a nossa vida como queremos, sem ser submetido ao escrutínio permanente dos nossos pares, dos nossos chefes, de todos aqueles que queiram submeter-nos e reduzir a nossa liberdade.

Porquê? Porque transforma a defesa de um direito fundamental numa suspeita, numa acusação, quase num crime, invertendo totalmente os valores em causa. Porque transforma a defesa de um direito numa infâmia. Porque insinua que quem protege a sua vida da devassa de outros, dos vizinhos, das empresas, dos patrões, das polícias, do Estado, dos sites da Internet, o faz porque comete ou cometeu actos inconfessáveis, ilegais, ilícitos, vergonhosos. Porque é uma posição que não compromete apenas aquele que a enuncia, mas contribui para definir um padrão social que irá limitar a liberdade de todos os outros.

Numa sociedade democrática (e não preciso de dizer democrática liberal porque a liberdade é condição da democracia, tem de estar na sua base, sem o que não há democracia) as pessoas têm direito a reservar a sua vida, diferentes aspectos da sua vida (aqueles que queiram, *à la carte*), do escrutínio de outros (aqueles que queiram, *à la carte*).

NÃO É SÓ A INTIMIDADE

É costume falarmos da "reserva da vida privada" e a Constituição da República Portuguesa defende o direito (artigo 26.º) "à reserva da intimidade da vida privada e familiar", mas não se trata apenas da "vida privada e familiar".

Para além deste *sanctum sanctorum* da nossa identidade, cuja devassa poucos hesitam em condenar, há inúmeros aspectos da nossa vida que, não sendo estritamente privados nem familiares, não nos importamos de revelar a uns mas queremos proteger do conhecimento de outros.

Uma pessoa pode frequentar aulas de *ballet* e, ainda que isso seja do domínio público no clube onde frequenta as aulas, que até podem ter assistência, pode querer manter isso em segredo dos seus colegas de trabalho. Outra pessoa pode querer manter em segredo de certas pessoas o seu emprego, porque o considera por alguma razão embaraçoso, mas este pode ser do domínio público num outro contexto. E a divulgação dessas informações no contexto errado poderia constituir uma violência imensa para a pessoa em causa, fonte de sofrimento, de culpa, vergonha, de possível coacção ou extorsão.

Todos conhecemos exemplos semelhantes e – mais significativamente – todos protegemos certas informações "não íntimas", "não privadas" e "não familiares" dos olhos de certas pessoas. Não porque sejam crimes ou sequer pecados, mas porque queremos moldar a *persona* que mostramos às pessoas com quem nos relacionamos. E temos esse direito. Todos mostramos diferentes personagens, diferentes *personas*, diferentes facetas a diferentes grupos e a diferentes pessoas. Não porque as queremos enganar, mas porque, tratando-se de pessoas diferentes, as tratamos como pessoas diferentes. Alguém conta as mesmas anedotas aos colegas da tropa e aos sogros? Alguém apresentará a mesma atitude nas reuniões do trabalho e quando fala ao namorado da filha? Será isso hipocrisia? Será isso um pecado? Ou será apenas o direito a exercermos a nossa liberdade de sermos diferentes conforme a circunstância, o interlocutor, o momento, o nosso objectivo nesse momento e a nossa história?

OS GRAUS DE CINZENTO E O CONTEXTO

A questão é que não existem de um lado dados que não nos importamos de revelar (públicos) e do outro lado dados que queremos preservar da observação dos outros (privados). A distinção não é tão clara e muito menos binária. Não é por acaso que discriminamos: dados familiares, pessoais, privados, íntimos. Informação sobre a nossa situação bancária, saúde, vida amorosa, sexualidade, sonhos. Existe um longo *continuum* entre estes dois mundos, público e privado, plenos de matizes e ramificações, de cinzentos infinitesimamente mais escuros ou mais claros.

E, para tornar tudo mais complexo, para cada informação não existe apenas o contexto de onde ela é originária, o contexto onde essa informação foi recolhida, o seu mundo de origem (saúde, finanças) mas o contexto em que ela é difundida, que muda tudo. Há informações absolutamente privadas num dado contexto, que constituiriam uma violência para a pessoa se fossem tornadas públicas nesse contexto, e que são partilhadas abertamente noutro grupo. A informação mais íntima, uma informação sobre a nossa saúde, sobre uma doença que nos aflige, que mantemos secreta do mundo, no nosso emprego, que podemos esconder até da nossa família e dos nossos amigos, pode ser partilhada num grupo de entre-ajuda de doentes, entre pessoas quase desconhecidas. A relação que mantemos com estas pessoas e com a nossa família é diferente e a faceta que queremos mostrar-lhes também.

Teremos esse direito? O direito de modular a informação sobre nós que permitimos que os outros consultem, que permitimos que os outros vejam? Penso que sim. Penso mesmo que essa deve ser a regra e que todas as invasões da nossa vida privada e todas as divulgações de dados pessoais devem ser as excepções, cuidadosamente e criteriosamente decididas. Felizmente, também a lei e a CNPD pensam, em geral, assim. E isso porque a relação de poder que temos com as diferentes pessoas com quem nos relacionamos é diferente. Há informação que receamos que possa ser, de alguma forma, usada contra nós num dado contexto e que não temos razão para recear difundir noutro contexto.

Colher informação num dado contexto e transplantá-la para outro – ou colher toda a informação que disponibilizamos voluntariamente "publicamente" nos vários contextos e disponibilizá-la em todos os outros contextos seria uma enorme violência. Seria literalmente despir a pessoa da sua persona e obrigá-la a exibir-se sem a roupa que escolheu para a sua vida social nos diferentes grupos a que pertence, nos diferentes mundos que frequenta.

EXPECTATIVA DE PRIVACIDADE

É por isso que, apesar de estarmos em público quando andamos numa rua, não é necessariamente aceitável, por esse simples facto, filmar as pessoas que passem nessa rua e muito menos divulgar essa informação publicamente.

Mesmo nos casos onde essa informação é recolhida – e deve haver um exigente escrutínio das razões para tal, dos benefícios dessa recolha e dos prejuízos possíveis – ela deve ser protegida tanto quanto possível, limitando as imagens colhidas, o tempo de arquivo e os acessos permitidos. E isto porque as pessoas têm, apesar de tudo, uma expectativa de relativa privacidade mesmo quando andam numa rua. A relativa privacidade que lhes é garantida pelo anonimato da cidade, da multidão, da hora de ponta, do lusco-fusco ou o que for e pelo facto de estar aqui e não estar ali (ou seja: de ter a expectativa de poder estar, eventualmente, a fornecer informação sobre a

sua localização a um determinado grupo de pessoas, as que se encontram na mesma rua, mas não ao mundo inteiro).

Se disséssemos a alguém que, sempre que passasse pela rua X, essa informação seria transmitida a todos os elementos da sua rede social, a toda a gente que a conhece ou conheceu, é provável que essa pessoa preferisse escolher outro trajecto. Não porque tencione fazer algo condenável na rua X, mas porque prefere não estar sob o foco da atenção alheia de milhares de pessoas. E tem esse direito. O direito ao anonimato, o direito a ser deixada em paz.

O SEGREDO É CONDIÇÃO DE LIBERDADE

A questão é que, quando estamos a ser escrutinados, observados, vigiados, não gozamos da mesma liberdade que quando nos julgamos fora do alcance da observação alheia. Agimos de maneira mais livre quando não somos vigiados, de maneira mais de acordo com o nossa verdadeira vontade, sem receio de críticas, admoestações, condenações, reparos, registo para eventual uso futuro. É por isso que o voto democrático é o voto secreto, o que podemos fazer sem que ninguém nos veja. É por isso que nos sentimos tão incomodados quando alguém espreita pelo buraco da fechadura, violando uma regra social que não parece muito relevante mas é, para todos, preciosa.

A verdade é que somos seres sociais mas somos, também, seres privados, indivíduos com uma mente secreta só nossa e esse espaço virtual de absoluta liberdade é essencial para sermos quem somos. Precisamos desse recato, da certeza de não estarmos a ser observados, para levar a cabo aquele diálogo connosco mesmos que define o nosso eu, os nossos pensamentos, que estrutura os nossos actos, que nos dá a coerência com a nossa história e as nossas ideias. Que escritor conseguiria escrever com alguém a espreitar por cima do seu ombro? Que compositor conseguiria compor? Quem conseguiria criar submetido a um escrutínio constante, a uma observação constante, por discreta e por benevolente que ela fosse? E isso não acontece porque se trate de obras secretas – o escritor e o compositor escrevem para o mundo - mas o momento da criação exige absoluta liberdade e a liberdade exige ausência de escrutínio, de observação alheia, respeito.

OS NOVOS VELHOS PROBLEMAS DA INTERNET

Transplantar a informação pessoal de um contexto para outro, de um tempo para outro, de um grupo para outro, foi algo que a Internet tornou constante. Porque a informação que se partilha nas redes sociais online é informação pessoal (quem sou, onde nasci, com quem namoro, como se chama o meu pai, onde passo férias, de que música gosto, onde estou neste momento e com quem e porquê) e porque toda essa informação, colhida em diferentes momentos, na companhia de diferentes pessoas, em diferentes contextos, é depois colocada num mesmo espaço onde fica para sempre, à mercê dos futuros utilizadores que não sabemos quem serão. É assim que o nosso patrão acede às fotografias da bebedeira que apanhámos em Porto Covo e fica a saber em que partido votámos nas últimas (e provavelmente também nas próximas) eleições. É assim que uma pessoa minimamente interessada que se dê ao trabalho fica a saber praticamente tudo sobre nós, esse conjunto de informações "públicas" que, devidamente articuladas, fazem um detalhadíssimo "retrato privado" da nossa vida.

É o que se chama o problema da "big data" e do respectivo "data mining", que coloca nas mãos de não sabemos quem, mais informações do que gostaríamos de lhes ter dado. Alterações no padrão do nosso comportamento (das compras que fazemos no supermercado, por exemplo) permitem a uma entidade com um software sofisticado e acesso aos dados (o nosso supermercado, por exemplo) saber algo que nem sequer contámos a ninguém: que estamos doentes, que estamos a fazer dieta, que estamos com problemas de dinheiro e talvez desempregados, que estamos apaixonados, que vamos ter um filho.

Há inúmeros problemas de privacidade nascidos com a Internet. Outro consiste no facto de que a maior parte dos utilizadores continua a pensar que a informação que disponibiliza (aos sites onde se inscreveu ou a outros utilizadores) apenas é vista pelo seu reduzido e simpático grupo de amigos. Sabem que não é assim, mas querem acreditar que é assim. Afinal, não têm nada a esconder, pois não?

Outro é o facto de que a maior parte dos utilizadores continua a pensar que a informação que disponibiliza na Internet desaparece no dia seguinte porque não está na última página do Face. Sabem que não é assim, mas querem acreditar que é assim.

E outro, maior, é o desaparecimento do tal contexto. Em vez de termos o grupo dos colegas, dos amigos do coração, das colegas do liceu, da malta da tropa, do grupo do judo, das amigas da avó, dos colegas da faculdade, que existem no mundo em diferentes mundos, a quilómetros de distância, a horas diferentes, a Internet é um único contexto, onde a avó sabe que patuscadas combinamos e o antigo namorado sabe que mudámos de emprego. Na Internet verifica-se o que chamo o *flattening* de todos os universos onde existimos - todos passam a ser apenas um. Todos se encontram no mesmo Facebook e o Twitter guarda as mensagens da noite para mostrar no dia seguinte a quem estava a dormir. O mesmo Facebook, o mesmo Twitter.

VELHO PROBLEMA, NOVAS SOLUÇÕES

Não é um enorme problema, mas obriga a uma nova aprendizagem por parte dos utilizadores. Uma aprendizagem que ainda não amadureceu e que, provavelmente, só vai emergir depois de algum sofrimento, como o caso de Justine Sacco, a directora de comunicação de uma grande empresa que descobriu, ao aterrar no país onde ia passar férias, que tinha sido despedida durante o voo por causa de um *tweet* que tinha enviado antes de o avião descolar e que o seu chefe considerou racista – assim como muitos milhares de pessoas que o difundiram pela rede, tornando a sua vida um inferno nos anos seguintes.

A Internet torna mais difícil compartimentar a nossa vida, como fazemos IRL (*in real life*). É fácil dizer, como dizem muitos (Scott McNealy, CEO da Sun; Mark Zuckerberg, CEO do Facebook) que a privacidade morreu e tudo o que temos a fazer é adaptarmo-nos a isso.

Não penso assim. É evidente que a Internet e as redes socias e a descoberta do valor comercial de certos dados (a nossa lista de compras) nos pressionaram a partilhar/difundir/desproteger muita informação, que hoje oferecemos sem pudor. É verdade que a tecnologia disponível permite hoje conhecer quase tudo sobre os cidadãos. É verdade que podemos saber muitas coisas uns sobre os outros que antes era difícil saber e que as empresas e outros poderes podem saber muito mais, quase tudo, com a possível excepção do que nos passa pela cabeça. Habituámo-nos a um certo grau de nudez, maior do que antes. Aquilo que queremos reservar mudou. Há *trade-offs* que estamos dispostos a fazer. Aquilo a que chamamos "vida privada" não é a mesma coisa a que chamávamos "vida privada" há vinte anos, tal como deixou de ser atrevido mostrar as pernas, mas a protecção da vida privada como conceito não perdeu actualidade, pelo contrário. É o direito a reservar aquilo que queremos reservar do escrutínio público. E aqui quem decide tem de continuar a ser a lei democrática, como tradução da moral, e não as possibilidades da tecnologia. Nem tudo o que é possível é desejável. Nem tudo o que é possível deve ser permitido. A vida privada tornou-se apenas um jardim mais difícil de cuidar. Mas é aí que está o cerne da nossa humanidade.

Texto escrito segundo a antiga ortografia


EM
FOCO

NOTAS SOBRE O REGIME SANCIONATÓRIO DA PROPOSTA DE REGULAMENTO GERAL SOBRE A PROTECÇÃO DE DADOS DO PARLAMENTO EUROPEU E DO CONSELHO

José Lobo Moutinho* e David Silva Ramalho**

*) Professor da Faculdade de Direito da Universidade Católica Portuguesa. Investigador do Católica Research Center for the *Future of Law*. Sócio da *Sérvulo & Associados*.

**) Mestrando na Faculdade de Direito da Universidade de Lisboa. Investigador do Centro de Investigação em Direito Penal e Ciências Criminais. Advogado na *Sérvulo & Associados*.

1. ENQUADRAMENTO PRÉVIO

Actualmente, a disposição de referência no Direito da União Europeia em matéria sancionatória relativa a infracções relacionadas com dados pessoais continua a ser a do artigo 24.º da Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, nos termos da qual «[o]*s Estados membros tomarão as medidas adequadas para assegurar a plena aplicação das disposições da presente directiva a determinarão, nomeadamente, as sanções a aplicar em caso de violação das disposições adoptadas nos termos da presente directiva*».

Para esta norma remetem, desde logo, o artigo 15.º, n.º 2, da Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas), bem como o artigo 13.º, n.º 1, da Directiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE[1].

Como é habitual em normas com este grau de indeterminação, a sua transposição para os diferentes ordenamentos jurídicos foi feita em termos significativamente distintos, quer quanto à qualificação da infracção como crime, contra-ordenação ou infracção punível com sanção administrativa, quer quanto à medida legal da sanção abstractamente aplicável.

1) Sendo certo que o objecto desta Directiva é substancialmente distinto do das outras, pois enquanto estas assentam no princípio de que o tratamento de dados pessoais deve estar sujeito a critérios de necessidade, pertinência e não excessividade em relação às concretas finalidades prosseguidas (sem prejuízo da excepção prevista no artigo 15.º, n.º 1, da Directiva 2002/58/CE), já a Directiva 2006/24/CE impõe a conservação de determinados dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas, tendo em vista garantir a disponibilidade desses dados para efeitos de investigação, de detecção e de repressão de crimes graves, tal como definidos no direito nacional de cada Estado membro. Foi, aliás, acima de tudo devido ao facto de esta Directiva impor uma significativa intromissão nos direitos fundamentais ao respeito pela vida privada e aos dados pessoais que o Tribunal de Justiça, no passado dia 8 de abril de 2014 (processos apensos C-293/12 e 594/12), a declarou inválida, por violação dos artigos 7.º, 8.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia - para uma análise da decisão de invalidade da Directiva, cf. Giuseppe Vaciago, «The Invalidation of the Data Retention Directive – A first impact assessment of the CJEU decisions in the joint cases C-293/12 and C-594/12», *Computer Law Review international*, n.º 3/2014, pp. 65-69.

Com efeito, a disparidade de tratamento e valoração destas infracções é, desde logo, visível dentro do próprio ordenamento jurídico português. Veja-se que, apesar de a norma que determina a aplicação de sanções por infracções em matéria de dados pessoais ser, como se viu, fundamentalmente a mesma nas referidas Directivas[2], a verdade é que, enquanto na Lei n.º 67/98, de 26 de Outubro, que transpõe para o ordenamento jurídico português a Directiva 95/46/CE, a coima máxima abstractamente aplicável mais elevada se situa nos € 29.927,87 (cfr. artigo 37.º, n.º 1, alínea *b)* e n.º 2), já na Lei n.º 41/2004, de 18 de Agosto, que transpõe para o ordenamento jurídico português a Directiva 2002/58/CE, prevêem-se sanções que ascendem aos € 5.000.000,00 (cfr. artigo 14.º, n.º 1).

É certo que para esta amplitude concorre também o facto de, entre a publicação de uma e outra lei, terem decorrido 6 anos, bem como a diferença dos âmbitos de incidência subjectiva de cada um dos diplomas[3]. Contudo, a verdade é que a sua vigência em simultâneo revela uma incongruência do sistema e denuncia diferentes graus de valoração de infracções que, no que aqui releva, têm por base essencialmente a violação de normas destinadas à protecção de dados pessoais.

Foi com o propósito declarado de estabelecer «*um quadro de protecção de dados sólido e mais coerente na União, apoiado por uma aplicação rigorosa das regras*», bem como «*sanções equivalentes para os infractores nos Estados membros*»[4] que a Comissão elaborou a Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, ou, mais abreviadamente, a Proposta de Regulamento Geral sobre Protecção de Dados[5].

O resultado, porém, peca por falta de clareza e presta-se às mais variadas interpretações, desde logo, e a título exemplificativo, quanto à aplicabilidade directa do Regulamento no que especificamente respeita à matéria sancionatória, quanto à qualificação das infracções aí previstas, quanto ao regime substantivo e processual subsidiariamente aplicável, bem como quanto às relações entre as normas do Regulamento e as normas nacionais actualmente vigentes.

2) Ainda que, em rigor, no caso da Directiva 2006/24/CE, para além da remissão para as disposições do capítulo III da Directiva 95/46/CE, nas quais se inclui a referida norma sobre sanções, exista ainda uma disposição autónoma igualmente sobre sanções, adaptada ao objecto específico da Directiva, nos termos da qual «[o]s *Estados membros devem tomar, em particular, as medidas necessárias para assegurar que o acesso ou a transferência intencional de dados conservados em conformidade com a presente directiva, não permitido pelo direito nacional adoptado em virtude da presente directiva, seja punível por sanções, incluindo sanções administrativas ou penais, que sejam efectivas, proporcionadas e dissuasivas*» (artigo 13.º, n.º 2).

3) Cabe recordar que a Lei n.º 41/2004 aplica-se ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações electrónicas acessíveis ao público em redes de comunicações públicas, nomeadamente nas redes públicas de comunicações que sirvam de suporte a dispositivos de recolha de dados e de identificação, pelo que se destinam, acima de tudo, a empresas que oferecem redes e ou serviços de comunicações electrónicas.

4) Cf. considerandos 5, 9 e 11 da Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a protecção de dados) – 2012/0011 COD).

5) Estima-se que a entrada em vigor do Regulamento e consequente desnecessidade de cumprimento de vários regimes distintos no espaço europeu, por parte de empresas multinacionais, permitirá uma poupança de cerca de 2.3 mil milhões de euros em encargos administrativos – cf. Viviane Reding, «The European data protecion framework for the twenty-first century», *International Data Privacy Law*, Vol. 2, n.º 3 (2012), p. 121.

2. APLICABILIDADE DIRECTA DO REGULAMENTO EM MATÉRIA SANCIONATÓRIA

Nos termos do disposto no 2.º parágrafo do artigo 288.º do TFUE, e como, aliás, consta da própria Proposta de Regulamento, este «[…] é obrigatório em todos os seus elementos e directamente aplicável em todos os *Estados membros*». Trata-se, portanto, de um acto legislativo da União Europeia, que, pela sua natureza, é parte integrante do direito interno e produz efeito directo simultaneamente nas relações verticais e horizontais, sem necessidade de qualquer mecanismo de recepção[6].

O motivo para a escolha deste acto jurídico, em detrimento, por hipótese, das habituais Directivas, pode ser encontrado na exposição de motivos da Proposta de Regulamento, na qual se refere que «[a] *sua aplicabilidade directa, prevista no artigo 288.º do TFUE, permitirá reduzir a fragmentação jurídica e proporcionar maior segurança jurídica, introduzindo um conjunto harmonizado de regras de base, melhorando a protecção dos direitos fundamentais das pessoas singulares e contribuindo para o bom funcionamento do mercado interno*»[7-8].

Contudo, em matéria sancionatória – precisamente aquela em que a segurança jurídica ganha maior importância –, o regime criado não permite sequer concluir, com clareza, se a Proposta de Regulamento, uma vez convertida em Regulamento, será directamente aplicável nesta matéria ou se implicará uma intervenção do legislador nacional, mormente pelos parlamentos nacionais.

Com efeito, dispõe o n.º 1 do artigo 78.º da Proposta de Regulamento, subordinado à epígrafe «*Sanções*» (em inglês, *penalties*), que «[o]*s Estados membros estabelecem as disposições relativas às sanções aplicáveis a infracções ao disposto no presente regulamento e tomam todas as medidas necessárias para assegurar a sua execução, incluindo quando o responsável pelo tratamento não respeitou a obrigação de designar um representante* […]». Por sua vez, dispõe o n.º 3 do mesmo artigo que «[c]*ada Estado membro notifica à Comissão as disposições do direito nacional que adoptar por força do n.º 1, o mais tardar na data fixada no artigo 91.º, n.º 2 e, sem demora, qualquer alteração subsequente das mesmas*».

---

6) Cf., por todos, Jónatas E. M. Machado, *Direito da União Europeia*, Coimbra: Coimbra Editora, 2010, pp. 199-201, e Miguel Gorjão-Henriques, *Direito da União Europeia*, Coimbra: Almedina, 7.ª ed., 2014, p. 296.

7) Cf. Exposição de motivos da proposta de Regulamento do Parlamento Europeu e do Conselho relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, COM(2012) 11 final, disponível em http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_pt.pdf.

8) Sendo certo que certas normas carecem de concretização legislativa por parte dos Estados membros, como sucede com o disposto no artigo 6.º, n.º 3, da Proposta, nos termos do qual o tratamento de dados pessoais com fundamento (i) na sua necessidade para o respeito de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito ou (ii) com fundamento na sua necessidade para o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento, deverá ser previsto pelo direito da União ou pela legislação do Estado membro à qual o responsável pelo tratamento está sujeito. O Parlamento Europeu acrescentou o seguinte excerto ao último parágrafo desta norma: «*[d]entro dos limites do presente regulamento, a legislação do Estado membro pode prever normas específicas aplicáveis à licitude do tratamento, em especial relativas ao responsável pelo tratamento, à finalidade e à limitação da finalidade do tratamento, ao tipo de dados e aos titulares dos dados, às operações e aos processos de tratamento, aos destinatários, assim como ao período de conservação*».

Da leitura das citadas disposições retirar-se-ia que, não obstante o Regulamento ser directamente aplicável a todos os Estados membros, as sanções aplicáveis em função da infracção daquelas normas deveriam ser objecto de previsão legal interna a criar pelos diversos Estados membros e a notificar à Comissão no prazo de dois anos[9].

No entanto, no artigo imediatamente seguinte, o artigo 79.º, subordinado à epígrafe «*Sanções administrativas*» (em inglês, *administrative sanctions*), deparamo-nos com uma tipificação, aparentemente taxativa, dos ilícitos administrativos decorrentes da infracção a disposições da Proposta de Regulamento, a que se segue a definição dos diferentes limites máximos das multas abstractamente aplicáveis, separados por categoria de infracção, em função da sua gravidade, e ainda os factores a ter em consideração na determinação da sanção a aplicar em concreto[10]. No n.º 2-A do mesmo artigo, introduzido no passado dia 12 de Março de 2014 pela emenda n.º 188 do Parlamento Europeu, refere-se inclusivamente que «[a] *autoridade de controlo impõe a quem não cumprir as obrigações previstas no presente regulamento, pelo menos uma das* […] *sanções*» aí enumeradas, nada se referindo quanto à necessidade de sucedâneo legal nacional para a aplicação ou para a definição destas sanções administrativas.

Perguntar-se-á, então, qual a diferença entre, por um lado, as *sanções* (*penalties*) referidas no artigo 78.º, cujas aplicação e concretização estão dependentes de base legal interna e, por outro lado, as *sanções administrativas* (*administrative sanctions*), con-

9) O que, de resto, em nada influenciaria a aplicabilidade directa do Regulamento nas demais matérias e em nada alteraria a natureza do acto legislativo escolhido. Como refere Miguel Gorjão-Henriques, a presunção de "autosuficiência normativa" de que gozam os Regulamentos, "*não implica que todo e cada regulamento seja em si mesmo preciso e suficiente, ao ponto de dispensar qualquer actuação normativa por parte da União ou dos Estados membros. É o que acontece, no primeiro caso, com os Regulamentos adoptados ao abrigo de processo legislativo e que prevêem a adopção de actos delegados ou de execução. E, no segundo caso, com aqueles (muitos) Regulamentos que, expressa ou implicitamente, habilitam os Estados membros a adoptar medidas de aplicação legislativas, regulamentares, administrativas e financeiras necessárias à sua efectiva aplicação, reconhecendo a estes, inclusivamente, poderes discricionários*" – cf. Miguel Gorjão-Henriques, *Direito*…, cit., p. 297.

10) «Sanções administrativas

1. Cada autoridade de controlo deve estar habilitada a aplicar sanções administrativas em conformidade com o presente artigo. As autoridades de controlo cooperam umas com as outras, nos termos dos artigos 46.º e 57.º, para garantir um nível harmonizado de sanções na União.

2. A sanção administrativa deve ser, em cada caso, efectiva, proporcionada e dissuasiva.

2-A. A autoridade de controlo impõe a quem não cumprir as obrigações previstas no presente regulamento, pelo menos, uma das seguintes sanções:

a) Uma advertência escrita, em caso de primeiro incumprimento, de carácter involuntário;

b) Auditorias periódicas regulares em matéria de dados;

c) Uma multa até 100 000 000 EUR ou, no caso de uma empresa, até 5 % do seu volume de negócios mundial anual, consoante o montante mais elevado»

2-B. Caso o responsável pelo tratamento ou o subcontratante seja detentor de um «Selo Europeu de Proteção de Dados» válido, nos termos do artigo 39.º, só será aplicada uma multa nos termos do n.º 2-A, alínea c), em caso de incumprimento voluntário ou negligente.

2-C. A sanção administrativa tem em conta os seguintes factores:

a) A natureza, a gravidade e a duração do incumprimento,

b) O carácter voluntário ou negligente da infracção,

c) O grau de responsabilidade da pessoa singular ou colectiva em causa e as infrações por ela anteriormente cometidas,

d) A natureza repetitiva da infracção,

e) O grau de cooperação com a autoridade de controlo, a fim de sanar a infracção e atenuar os seus eventuais efeitos negativos,

f) As categorias específicas de dados pessoais afectadas pela infracção,

(g) O nível de prejuízo, inclusive de natureza não-pecuniária, sofrido pelos titulares dos dados,

(h) As medidas tomadas pelo responsável pelo tratamento ou pelo subcontratante para atenuar o prejuízo sofrido pelos titulares dos dados,

(i) Os eventuais benefícios financeiros visados ou obtidos ou as perdas evitadas, directa ou indirectamente, por intermédio da infracção,

(j) O grau das medidas e dos procedimentos técnicos e organizacionais postos em execução […]»

sagradas no artigo 79.º da Proposta de Regulamento, para as quais, aparentemente, não é necessária semelhante adaptação legislativa?

O legislador da União não esclarece.

Perguntar-se-á: qual o sentido de o legislador da União, por um lado remeter para o legislador nacional a definição da sanção (*penalty*) aplicável a uma certa infracção e, por outro, definir o valor máximo da sanção administrativa (*administrative sanction*) aplicável pela sua prática, especialmente tendo em conta que este valor máximo, por decorrer de Regulamento da UE, não pode ser modificado por iniciativa do legislador nacional?

Poderá dar-se o caso, como alguns vêm avançando[11], de as sanções a que se refere o artigo 78.º revestirem natureza criminal, assim carecendo de consagração legal interna, ao passo que as do artigo 79.º revestiriam somente natureza administrativa?

A favor deste entendimento podem encontrar-se alguns argumentos.

Em primeiro lugar, começar-se-á por referir que as alterações ao Considerando 119, bem como a adição do novo Considerando 119a à Proposta de Regulamento, ambas introduzidas pelo Parlamento Europeu, por via da sua resolução de 12 de Março de 2014, vieram prever expressamente que as regras sobre sanções (leia-se, *penalties*) e respectiva aplicação «*devem ser objecto de salvaguardas processuais adequadas, de acordo com os princípios gerais do Direito da União e da Carta dos Direitos Fundamentais, incluindo o direito à tutela jurisdicional efectiva, a um processo equitativo e o princípio do* ne bis in idem». Esta nova previsão clarifica, num primeiro momento, que as sanções a que se refere o artigo 78.º revestem cariz punitivo *stricto sensu* e não se traduzem em meras consequências de carácter civil, como sucede, por exemplo, com aquilo a que em actos legislativos da União por vezes se classifica como *sanção civil* ou *sanção de nulidade*. A este facto acresce que a previsão da necessidade de imposição de *salvaguardas processuais adequadas* apenas é feita em relação às sanções (*penalties*) e não às sanções administrativas (*administrative sanctions*), de onde é legítimo concluir que aquelas revestirão maior gravidade.

Por outro lado, haverá que ter em atenção que a introdução destes novos Considerandos aparenta consubstanciar um *conselho* dirigido pela UE às instâncias nacionais, para que estas determinem a sua conduta dentro dos limites estabelecidos pela própria UE. Assim, a UE actua estabelecendo as regras aplicáveis e, na parte em que confere liberdade de actuação a outras instâncias, dirige-lhes directrizes para que estas norteiem a sua conduta de acordo com a vontade do legislador da UE. Deste modo se explicaria o facto de a União conjugar a margem de liberdade legislativa conferida aos Estados membros em matéria sancionatória no artigo

11) Assim, Yann Padova, «What the European Draft Regulation on Personal Data is going to change for companies», *International Data Privacy Law*, 2014, Vol. 4, no. 1, p. 44; e ainda o *Article-by-article research Paper do Information Comissioner's Office*, disponível em: http://ico.org.uk/news/~/media/documents/library/Data_Protection/Research_and_reports/ico_proposed_dp_regulation_analysis_paper_20130212_pdf.ashx.

78.º com esta advertência da necessidade de criação das *salvaguardas processuais adequadas* aquando da sua utilização. Veja-se que a UE não prevê semelhante regra em relação às sanções administrativas, apesar de as mesmas também estarem, naturalmente, sujeitas aos princípios gerais da legislação da União e da Carta dos Direitos Fundamentais da União Europeia, incluindo as relativas ao direito a um efectivo recurso judicial, a um processo adequado e ao princípio *ne bis in idem*[12] (cfr. considerando 119). E não o faz, cremos, não tanto ou não só por estas revestirem menor gravidade (pelo menos formalmente), mas também e sobretudo porque nesta matéria é a própria União quem estabelece as normas directamente aplicáveis, inexistindo qualquer *risco* de o legislador nacional não respeitar estes princípios. Quando, porém, é conferida alguma liberdade de actuação a instâncias exteriores à União – leia-se, quando a aplicação das normas de fonte europeia tem de ser *confiada* a outras entidades –, como sejam as autoridades de controlo que aplicam estas sanções administrativas, já a União lhes dirige uma advertência, no Considerando 120 e no recente n.º 2-C do artigo 79.º, dando instruções quanto aos factores a ter em consideração no cálculo da multa a aplicar em concreto.

É certo que o facto de as sanções administrativas também carecerem de *salvaguardas processuais adequadas* poderia abrir caminho ao argumento de que a sua previsão apenas quanto às sanções (*penalties*) significaria que estas englobariam as sanções administrativas. Contudo, tal entendimento soçobraria perante a constatação da existência de dois artigos diferentes, nos quais se aplica terminologia também diferente (*penalties* e *administrative sanctions*), a qual é replicada nos Considerandos em locais separados, sendo que num dos artigos se remete a densificação para instrumento legal nacional e noutro se procede à densificação no próprio Regulamento. A favor deste entendimento, ainda que tratando-se de um argumento meramente linguístico, milita a dicotomia sanção penal/administrativa adoptada nas versões francesa (*Sanctions pénales/sanctions administratives*) e eslovena (*Kazenske sankcije/Upravne sankcije*) das epígrafes dos artigos 78.º e 79.º do Regulamento.

Acresce que a aplicabilidade directa destas normas sancionatórias, sem necessidade de mediação nacional, é a única opção que se revela consentânea com a escolha de um Regulamento em detrimento de uma Directiva, pois é a única que garante a tão procurada segurança jurídica. Assim se fixa uma base legal uniforme a nível da União que estabelecerá coordenadas idênticas nos diversos Estados membros para que as diferentes autoridades de controlo decidam em conformidade. Sendo certo que, quando, em concreto, a sanção aplicada por uma autoridade de controlo nacional distar daquela aplicada noutro Estado membro, tendo por base a mesma norma, haverá lugar ao recurso ao mecanismo de controlo da coerência, previsto nos artigos 57.º e seguintes da Proposta de Regulamento – cf. novo segundo período do artigo 79.º, n.º 1.

12) Sobre este tema cfr. Vânia Costa Ramos, *Ne bis in idem e União Europeia*, Coimbra: Coimbra editora, 2009, pp. 212-216.

Mais, os ilícitos tipificados no artigo 79.º puníveis com sanções administrativas assentam numa lógica de remissão para deveres previstos ao longo do Regulamento. A imposição de transposição destes dispositivos de cariz sancionatório para os ordenamentos jurídicos nacionais implicaria a transposição dos deveres cujo incumprimento aquelas normas declaram punível – o que, em última análise, poderia levar a uma transposição quase integral do Regulamento ou à necessidade de estabelecer normas sancionatórias nacionais por remissão para deveres Regulamentares, quando existem normas idênticas no próprio Regulamento.

Assim, e embora tal solução não seja clara, afigura-se-nos que a intenção do legislador da União foi a de permitir a aplicação directa e uniforme dos ilícitos punidos com sanções administrativas previstos no artigo 79.º da Proposta de Regulamento, destacando-os das infracções puníveis com as sanções previstas no artigo 78.º, às quais pretenderá ver atribuída uma natureza ou configuração criminal.

3. QUALIFICAÇÃO DAS INFRACÇÕES E CONCURSO DE NORMAS

Admitir a aplicação directa das sanções administrativas por força do Regulamento está muito longe de resolver todos os problemas.

Entre nós, surge, desde logo, uma questão de base da maior relevância: como qualificar estas sanções e as infracções a que correspondem?

Sendo o critério para a definição de crime e de contra-ordenação, um critério formal, ou até nominal[13] – no primeiro caso, a prática de um facto declarado passível de *pena* por lei (artigo 1.º, n.º 1, do Código Penal), e, no segundo, a prática de um facto que preencha um tipo legal no qual se comine uma *coima* (artigo 1.º do RGCO)[14] –, seremos forçados a concluir que nos encontramos perante um *tertium genus*, desde logo porque o conceito de *sanção administrativa* – até possivelmente não pecuniária, por força das novas alíneas *a)* e *b)* do n.º 2-A do artigo 79.º do Regulamento – não permite enquadrar imediatamente as infracções a que se reporta no conceito de crime ou de contra-ordena-

13) Assim, «*[n]a realidade, bem vistas as coisas estamos perante a adopção dum critério simplesmente nominal. É que para, por seu turno, se apurar quando estamos perante uma coima não parece bastar uma mera equivalência de natureza (sanção pecuniária não convertível em prisão), como demonstram os casos, não só das multas disciplinares, como das multas processuais e das multas aplicáveis às pessoas colectivas em caso de crime. Tudo vem, pois, a depender do facto de o tecto da lei conter a palavra "coima" para designar a sanção correspondente ao facto ilícito. A opção por um critério nominal é, sem dúvida, de entre todas, a mais pragmática, na medida em que poupa o intérprete à questão da qualificação.*» - Cfr. José Lobo Moutinho, *Direito das contra-ordenações – Ensinar e investigar*, Lisboa: Universidade Católica Editora, 2008, pp. 29-30.

14) Daí que, como refere Cavaleiro de Ferreira, *"[a] regulamentação das «contra-ordenações», por referência ao Direito Penal, mostra que é impossível deixar de ver nas «contra-ordenações» o que elas efectivamente são – infracções penais administrativas. A renúncia da lei a fixar uma distinção material delimitando de maneira nominal crime e «contra-ordenação» confirma o juízo que fica formulado»*, em *Direito Penal Português I*, Lisboa: Verbo, 1982, p. 17.

ção[15]. Conclusão a que, aliás, sempre chegaríamos pela reserva relativa de competência legislativa da Assembleia da República em matéria penal e contra-ordenacional – neste último caso, desde que se introduza desvio ao RGCO, como sucede a todo o passo com o regime estabelecido no Regulamento, a começar logo com os limites das sanções previstas no Regulamento, que, por um lado excedem largamente os limites do artigo 17.º do RGCO[16], e por outro, ao não incluírem limites mínimos, admitem a interpretação segundo a qual permitem implicitamente a existência de limites mínimos inferiores aos estabelecidos no mesmo artigo –, reserva que é, a nosso ver, insusceptível de ser afastada nesta matéria, por aplicação directa de um instrumento jurídico da União Europeia.

É certo que nada obriga a que as infracções existentes no ordenamento jurídico português sejam qualificadas como crimes ou contra-ordenações. Basta pensar no regime da responsabilidade sancionatória do Tribunal de Contas, ou mesmo na infracção administrativa punível com multa, prevista no artigo 130.º, n.º 2, da Lei do Jogo[17], para logo nos apercebermos de que, na nossa ordem jurídica, há ilícitos para os quais se prevê a aplicação de multas, sem que as respectivas infracções sejam qualificadas, ou qualificáveis, como crimes ou contra-ordenações.

Todavia, a questão da qualificação das infracções previstas na Proposta de Regulamento numa das referidas categorias não é despicienda. Por um lado, ela serve para determinar o regime substantivo e processual geral ou subsidiariamente aplicável que, em domínios sancionatórios avessos à integração de lacunas *in malam partem*, permita fazer face ao amplo espaço deixado em aberto pela Proposta de Regulamento. Por outro lado, a qualificação é essencial para estabelecer com clareza a complexa questão da relação entre as normas sancionatórias actualmente vigentes e as que venham a constar do Regulamento, de acordo com a respectiva proposta.

Na verdade, com a entrada em vigor do Regulamento, e admitindo, em benefício da discussão, a aplicação directa das suas normas que prevêem a aplicação de sanções administrativas, pergunta-se: poderá o Regulamento revogar tacitamente normas legais nacionais que prevêem ilícitos contra-ordenacionais, ou poderão as normas coexistir, duplicando a punição por infracções que, na sua estrutura real e no seu desvalor, são substancialmente as mesmas[18]? Temos dúvidas quanto à admissibilidade da primeira hipótese e certeza quanto à inconstitucionalidade da segunda.

---

15) Sendo certo que certas contra-ordenações podem não implicar a aplicação de uma coima, como sucede no artigo 15.º, n.º 2, da Lei n.º 30/2000, de 29 de Novembro, que aprova o Regime Jurídico do Consumo de Estupefacientes, nos termos do qual «*[a]os consumidores toxicodependentes são aplicáveis sanções não pecuniárias*» - sobre este tema v. Alexandra vilela, *O Direito de Mera Ordenação Social – Entre a Ideia de "Recorrência" e a de "Erosão" do Direito Penal Clássico*, Coimbra: Coimbra Editora, 2013, pp. 369-371.

16) Sobre este assunto, v., por todos, acórdão do TC n.º 447/91, disponível em www.tribunalconstitucional.pt.

17) Cfr. Paulo Pinto de Albuquerque, *Comentário do Regime Geral das Contra-Ordenações,* Lisboa: Universidade Católica Editora, 2011, p. 27.

18) Referindo-se inicialmente ao acórdão Simmenthal, de 9 de Março de 1978, refere Jónatas E. M. Machado que «*[d]e acordo com esta última decisão, o juiz nacional deve aplicar, por sua própria autoridade, o direito comunitário, desaplicando, se necessário, a norma de direito interno que entre em contradição com aquele, mesmo que se trate de uma norma posterior. Para isso, não se torna necessário pedir ou aguardar a prévia revogação da norma de direito interno, seja por via de procedimento legislativo, seja através de procedimento constituinte. No entanto, constitui um dever dos Estados a revogação expressa das normas internas incompatíveis com normas comunitárias*" – em *Direito…*, cit., p. 227.

E se a norma do Regulamento sancionar administrativamente uma conduta simultaneamente tipificada como crime no ordenamento jurídico nacional, como pode suceder, por exemplo, com a violação do dever de guardar sigilo profissional, nos termos do disposto no artigo 79.º, n.º 6, alínea *o)* do Regulamento e do artigo 47.º da Lei n.º 67/98, respectivamente?

Deverá aplicar analogicamente o disposto no artigo 39.º, n.º 1, da Lei n.º 67/98, subordinado à epígrafe «*Concurso de infracções*», nos termos do qual «[s]*e o mesmo facto constituir, simultaneamente, crime e contra-ordenação, o agente é punido sempre a título de crime*»[19]? Ou, pelo contrário, deverá concluir-se pela punição simultânea e a ambos os títulos da mesma infracção? Novamente, temos dúvidas quanto à admissibilidade da primeira e a certeza quanto à inconstitucionalidade da segunda.

É que, como o Tribunal Constitucional tem considerado, tanto em matéria daquilo a que tradicionalmente se tem chamado concurso ideal de crimes, como em matéria de concurso entre crime e contra-ordenação, não havendo uma diferença ao nível do bem jurídico protegido, a punição por ambas as infracções viola o *ne bis in idem* substantivo[20].

4. OS RESPONSÁVEIS PELAS INFRACÇÕES

Outras dúvidas que se colocam a propósito do regime sancionatório estabelecido pela proposta de Regulamento prendem-se com o seu âmbito de incidência subjectiva.

Por um lado, no artigo 4.º, n.os 15 e 16, o Regulamento apresenta as definições de empresa (*enterprise*) e grupo de empresas (*group of undertakings*). Assim, a empresa é definida como «*qualquer entidade que, independentemente da sua forma jurídica exerce uma actividade económica, incluindo, nomeadamente, as pessoas singulares e colectivas, as sociedades ou associações que exercem regularmente uma actividade económica*», enquanto o grupo de empresas é definido como «*um grupo composto pela empresa que exerce o controlo e pelas empresas controladas*», sendo que, de acordo com o Considerando n.º 28 da Proposta de Regulamento, a empresa que exerce o controlo é «*aquela que pode exercer uma influência dominante sobre as outras empresas, por exemplo, em virtude da propriedade, participação financeira ou das regras que a regem ou da faculdade de fazer aplicar as regras relativas à protecção de dados pessoais*».

Acontece que, quando, no artigo 79.º, n.os 4, 5 e 6 da Proposta de Regulamento, o legislador da União delimita o *quantum* das sanções administrativas pecuniárias abstractamente aplicáveis, fixa-as em função da percentagem do volume de negócios mundial anual da empresa (*enterprise*), nada dizendo quanto aos grupos de empresas (*group of undertakings*).

19) Disposição que, de resto, reproduz quase integralmente o disposto no artigo 20.º do RGCO.

20) Cfr. Acórdãos do TC nos 244/99, 303/05 e 375/2005, disponíveis em www.tribunalconstitucional.pt.

A conjugação do disposto neste artigo com as definições de *empresa* e de *grupo de empresas supra* referidas suscita a dúvida de saber se o volume de negócios mundial anual da empresa que releva no cálculo da sanção deverá ou não ter em consideração o volume de negócios de outras empresas com as quais esta tenha relação, designadamente com a empresa que eventualmente exerça o controlo sobre a empresa a quem se imputa a infracção ou com uma sociedade *irmã*. Ou seja: se a *empresa* a quem se imputa a infracção, não obstante ser dotada de personalidade jurídica, for simplesmente uma empresa integrada num grupo multinacional e, consequentemente, for dominada por outra empresa, será sustentável o entendimento segundo o qual o cálculo do volume de negócios mundial anual poderá traduzir-se no volume de negócios nacional desta empresa, descurando o volume de negócios das demais empresas com as quais se encontre ligada?

Uma segunda dúvida que se suscita é relativa à questão de saber a quem se aplicam as sanções administrativas quando estejamos perante uma entidade responsável pelo tratamento de dados de cidadãos da União Europeia que não esteja estabelecida no território da União, nos termos do disposto no artigo 3.º, n.º 2, da Proposta de Regulamento.

A este respeito refere o artigo 78.º, n.º 2, da Proposta de Regulamento que «[s]*empre que o responsável pelo tratamento tiver designado um representante, as sanções são aplicadas ao representante, sem prejuízo de quaisquer sanções que possam vir a ser aplicadas ao responsável pelo tratamento*». Contudo, como se viu, não é claro que as sanções contempladas no artigo 78.º englobem as sanções administrativas a que se refere o artigo 79.º, pelo que, a concluir-se pela existência de uma distinção estanque entre ambas, a norma que permite imputar a *sanção* ao representante não será aplicável às *sanções administrativas*, ficando estas sujeitas ao regime geral de aplicação directamente ao responsável pelo tratamento.

5. SANÇÕES

Uma das principais alterações que, de acordo com a Proposta, o Regulamento virá introduzir prende-se com o montante das sanções administrativas aplicáveis a infracções de normas relativas a protecção de dados, muitas vezes traduzidas no mero e potencialmente inconsequente incumprimento de formalidades.

Com efeito, de uma ausência de determinação no seio da União Europeia dos montantes sancionatórios aplicáveis passámos para a criação de um catálogo de infracções às quais são associadas molduras sancionatórias que atingem o valor de € 1.000.000 ou 2% do volume de negócios mundial anual da empresa. Entre as infracções que atingem esta moldura sancionatória máxima abstractamente aplicável encontra-se, por exemplo, no artigo 79.º, n.º 6, alínea *e)*, a violação – meramente procedimental[21],

21) Peter Traung fala aqui de «mere paperwork sanctions» em «The Proposed New EU General Data Protection Regulation», *Computer Law Review international*, 2/2012, pp. 40 (n. 63), 43, 44 e 47.

note-se – da obrigação de adoptar regras internas ou a não execução de medidas adequadas para assegurar e comprovar o respeito das obrigações previstas nos artigos 22.º, 23.º e 30.º do Regulamento. A tipificação de infracções de dever como esta, destituídas de resultado material, no escalão máximo sancionatório aplicável, cria um abismo entre, por um lado, a gravidade da infracção e a culpa do agente da infracção, inseparável da consciência do desvalor do ilícito e mensurável em função do grau de motivação necessário para o desvio à norma, e, por outro, a consequência imposta por força da conduta praticada.

Acresce que, com as alterações efectuadas pelo Parlamento Europeu em 12 de Março de 2014, passou a prever-se, no novo n.º 2-A, alínea *c*), do artigo 79.º, a possibilidade de a autoridade de controlo impor uma multa no valor máximo de € 100.000.000 ou 5% do volume de negócios mundial anual da empresa. A introdução desta previsão foi, porém, desacompanhada da referência a tipos legais aos quais uma tal sanção pudesse ser aplicada, pelo que desconhecemos em que casos poderá esta moldura sancionatória ser aplicável ou se é intenção do legislador da União permitir que os parlamentos nacionais as associem livremente às infracções que entenderem.

Deve ainda assinalar-se que a introdução em Março de 2014, deste n.º 2-A, foi acompanhada da reformulação do n.º 6 do artigo 79.º, nos termos do qual passou a prever-se que «[s]ão atribuídas competências à comissão para adoptar actos delegados *em conformidade com o artigo 86.º, a fim de actualizar os montantes absolutos das multas administrativas referidas no parágrafo 2-A, tendo em consideração os critérios e factores referidos nos parágrafos 2 e 2-C*».

Ora, estes actos delegados, de acordo com o disposto no artigo 290.º do TFUE, conferem à Comissão o poder de adoptar actos que completem ou alterem elementos não essenciais de um acto legislativo. Daqui se retira que o legislador, por via desta norma, conferiu à Comissão o poder de, *motu proprio*, aumentar o montante máximo sancionatório abstractamente aplicável, fixado em € 100.000.000, sem necessidade de qualquer acto legislativo ulterior, considerando o montante da sanção aplicável como um elemento *não essencial* da norma.

Com efeito, se o legislador age, nas palavras de Beccaria, como o «*hábil arquitecto cujo ofício é o de se opor às direc*ções desastrosas *da* [força da] *gravidade e de consolidar aquelas que contribuem para a segurança da construção*»[22], diríamos que a União Europeia criou um edifício cuja excessiva solidez não se adaptará às forças das Constituições nacionais e ruirá sobre si mesma.

Acresce que o Regulamento conjugou a criação de um limite máximo sancionatório abstractamente aplicável de 100.000.000€ ou 5% do volume de negócios mundial anual da empresa, com uma ausência de limites mínimos às sanções abstractamente aplicáveis que prevê. Para além de problemas de proporcionalidade, na medida em

22) Cesare Beccaria, *Dos delitos e das penas*, Lisboa: Fundação Calouste Gulbenkian, 3.ª ed., 2009, p. 73.

que a infracções de ínfima gravidade possam fazer-se seguir sanções de gravidade inversamente severas, este regime suscita um patente problema de legalidade. Na verdade, a experiência constitucional portuguesa em matéria de contra-ordenações ensina que o princípio da determinação das sanções, como momento do princípio da legalidade estabelecido no artigo 29.º da Constituição, não é aplicável apenas no Direito Penal ou Criminal, mas ainda noutros Direitos Sancionatórios, como momento fundamental de tutela da pessoa perante o Estado (mormente, o Estado-Administração) no exercício do seu temível poder de punir e que, nessa vertente, se enquadra logo a proscrição de sanções com limites tão distantes entre si que traduziriam a transferência da função legislativa (ou normativa) para o aplicador da sanção e, portanto, a ausência de qualquer garantia contra o arbítrio. E tem se de acrescentar que, se é certo que a jurisprudência do Tribunal Constitucional mostra divergências a respeito da concretização dessa exigência[23], não é menos verdade que, tal qual resultam da Proposta de Regulamento, as sanções em causa não se mostram aptas a resistir às exigências de nenhuma das várias orientações assumidas pelo Tribunal Constitucional.

6. QUESTÕES DE DIREITO PROCESSUAL

Em matéria processual, não se afiguram particularmente significativas as alterações levadas a cabo pelo novo Regulamento, quando comparadas com o regime contra-ordenacional português vigente – para todos os efeitos, o regime mais próximo do enquadramento sancionatório adoptado pela Comissão – inclusivamente em matéria de protecção de dados.

Quanto ao direito de queixa previsto no artigo 73.º do Regulamento, nos termos do qual «[s]*em prejuízo de qualquer outra via de recurso administrativo ou judicial, todos os titulares de dados têm o direito de apresentar queixa a uma autoridade de controlo em qualquer Estado membro se considerarem que o tratamento dos seus dados pessoais não respeita o presente regulamento*», verifica-se que o mesmo nada parece trazer de novo relativamente ao regime das contra-ordenações.

Estamos, é certo, perante um uso impróprio do termo "*queixa*", pois, em rigor, esta, embora envolva naturalmente a notícia de uma infracção, é uma declaração de vontade de procedimento necessária nos casos em que o procedimento dependa dessa vontade (como sucede nos crimes semi-públicos e particulares). Mas essa impropriedade existe já hoje no regime vigente em matéria de protecção de dados, em particular no do artigo 33.º da Lei n.º 67/98 e do artigo 17.º da Lei de Organização e Funcionamento da Comissão Nacional de Protecção de Dados, aprovada pela Lei n.º 43/2004, de 18 de Agosto, que prevê a apresentação de "queixas" à CNPD, a quem competirá aplicar as coimas correspondentes, em caso de verificação da prática de uma infracção. E as contra-ordenações são infracções de natureza pública (cfr. artigos 54.º, n.º 1, e 48.º do RGCO), em relação às quais vigora o princípio da legalidade processual (artigo 43.º do RGCO).

23) Cfr. Acs. TC n.º 574/95, 547/01 e 41/2004.

No que concerne ao chamado direito de acção judicial contra decisões de uma autoridade de controlo, previsto no artigo 74.º do Regulamento, e mesmo cingindo a análise às decisões no âmbito do exercício dos poderes sancionatórios, importa distinguir. Relativamente a decisões interlocutórias, ou seja, decisões, despachos e demais medidas tomadas pelas autoridades administrativas no decurso do processo sancionatório, parece não haver novidade significativa em relação ao regime estabelecido no artigo 55.º do RGCO, que permite o recurso de medidas de autoridades administrativas que colidam *"com os direitos ou interesses das pessoas"* (artigo 55.º, n.º 2). Mas o regime previsto, ao consagrar, aparentemente como princípio geral, que "[s]*em prejuízo de qualquer outra acção administrativa ou extrajudicial, qualquer pessoa singular ou colectiva tem direito de acção judicial contra todas as decisões de uma autoridade judicial que lhe digam respeito*" (artigo 74.º, n.º 1), parece querer ir muito mais longe. Por um lado, parece consagrar-se um direito de accionar judicialmente a autoridade de controlo, em detrimento do direito de recorrer judicialmente de decisões proferidas pela autoridade de controlo. Por outro lado, mesmo no seio do processo sancionatório, aquele geral direito de acção tem consequências.

À uma, naquilo que, relativamente ao regime actual e também ao RGCO, constitui novidade, consagra-se a impugnação da não abertura de processo na sequência de queixa (artigo 74.º, n.º 2 ss.), a qual, de certo modo, pode encontrar um antecedente em Portugal no regime de processamento de denúncias, estabelecido no artigo 8.º, n.os 2 e 4, do Regime Jurídico da Concorrência, aprovado pelo Lei n.º 19/2012, de 8 de Maio.

À outra, contudo, fica a dúvida de saber se o genérico direito de acção, na vertente de direito à impugnação, não irá além disso, abrangendo também as decisões finais, condenatórias ou de arquivamento, permitindo o seu exercício, assim, a qualquer pessoa a quem essas decisões "digam respeito". Uma tal solução mostrar-se-ia em absoluto incompatível com a estrutura do nosso processo de contra-ordenações, que só admite a impugnação da decisão condenatória pelo arguido ou pelo seu defensor (artigo 59.º, n.os 1 e 2, do RGCO), fazendo-lhe seguir uma fase híbrida, em que a decisão administrativa se convola em acusação (artigo 62.º, n.º 1, do RGCO).

Referência merece, finalmente, a admissão da figura da advertência, no caso de uma primeira e não intencional inobservância do regulamento. Dentro das duas figuras diversas que o nosso ordenamento tem confundido debaixo da designação "advertência", estaremos perante algo que é mais próximo da *admoestação* prevista no artigo 51.º do RGCO do que de uma verdadeira *advertência* prevista em certos domínios para casos de irregularidade sanável que ainda não tenha produzido danos significativos, como alternativa à instauração do processo de contra-ordenações.

Em qualquer caso, a previsão da sua aplicação a qualquer infracção ao Regulamento confirmam ou até adensam as dúvidas atrás suscitadas, relativamente à proporcionalidade e à determinação das gravíssimas sanções previstas na Proposta de Regulamento.

7. FASES SEGUINTES DO PROCESSO LEGISLATIVO

O presente processo legislativo ordinário foi iniciado pela apresentação da proposta de Regulamento, por parte da Comissão, ao Parlamento Europeu e ao Conselho[24], a que se seguiu, no dia 12 de Março de 2014, a primeira leitura do Parlamento Europeu, na qual foram efectuadas 205 propostas de alteração ao texto original[25].

Segue-se agora a primeira leitura do Conselho, na qual este poderá aprovar a posição do Parlamento Europeu[26], caso em que a proposta será adoptada com as propostas de alteração introduzidas em Março, ou pode não aprovar a referida posição e adoptar a sua própria posição para subsequente envio ao Parlamento Europeu para segunda leitura[27].

A segunda leitura permite ao Parlamento Europeu (i) aceitar os motivos de desacordo apresentados pelo Conselho em primeira leitura – aqui com um prazo de três meses, prorrogável por um mês –, caso em que a proposta será aprovada com a formulação dada pelo Conselho; (ii) rejeitar a posição do Conselho, por maioria dos deputados, assim inviabilizando a adopção do acto; ou (iii) propor emendas à posição do Conselho[28].

Na eventualidade de serem apresentadas emendas por parte do Parlamento Europeu, poderá o Conselho aceitá-las, caso em que o acto será aprovado nos termos propostos por aquele órgão, ou rejeitá-las, caso em que se segue uma tentativa de conciliação[29].

Caso se prossiga para a tentativa de conciliação, será convocado um Comité de Conciliação, por parte do Presidente do Parlamento Europeu, composto por membros do Conselho, ou seus representantes, e por membros do Parlamento Europeu, em igual número, que deverá chegar a um acordo, num prazo de seis semanas, prorrogável por mais duas, sob pena de o acto não ser aprovado[30].

Caso haja acordo, haverá então lugar a uma terceira leitura, desta feita do projecto comum do Comité de Conciliação, que deverá ser aceite por maioria qualificada do Conselho e maioria do Parlamento Europeu, no prazo de seis semanas[31].

Seguir-se-á a sua assinatura por parte dos presidentes do Parlamento Europeu e do Conselho, seguida da sua publicação no Jornal Oficial da União Europeia[32].

24) Cf. artigo 294.º, n.º 2, do TFUE.
25) Cf. artigo 294.º, n.º 3, do TFUE.
26) Cf. artigo 294.º, n.º 4, do TFUE.
27) Cf. artigo 294.º, n.º 5, do TFUE.
28) Cf. artigo 294.º, n.º 7, do TFUE.
29) Cf. artigo 294.º, n.º 8, do TFUE.
30) Cf. artigo 294.º, n.ºs 10 a 12, do TFUE.
31) Cf. artigo 294.º, n.ºs 13 e 14, do TFUE.
32) Cf. artigo 297.º, n.º 1, do TFUE.

O Regulamento entrará em vigor no vigésimo dia seguinte ao da sua publicação, mas apenas será aplicável passados dois anos daquela data[33]. Em face do actual estado do processo legislativo, não é, portanto, expectável que o Regulamento entre em vigor em 2016, como inicialmente esperado.

8. CONCLUSÕES

De quanto se expôs conclui-se que o legislador da União foi demasiado ambicioso na sua pretensão de uniformização das normas vigentes em matéria sancionatória por violação de normas relativas a dados pessoais.

Ao fazê-lo, deixou questões importantíssimas por resolver que, a não serem corrigidas até à entrada em vigor do Regulamento, criarão sérias dificuldades interpretativas e, consequentemente, terão o efeito inverso ao pretendido: a criação de insegurança jurídica.

A tutela sancionatória carece de ser cuidadamente (re)pensada e (re)definida, tendo em atenção a natureza das infracções em causa. Com efeito, a tutela dos bens jurídicos subjacentes à protecção de dados não se cria pela imposição externa de sanções desproporcionais ao agente da infracção, num pensamento, afinal, de uma prevenção geral entendida de forma bastante primária, devendo ser antes o fruto de um labor de sensibilização que faça brotar da consciência jurídica comum a compreensão dos referidos valores e a importância do seu respeito para tutela da pessoa humana no que é a realidade da vida social e comunicacional dos nossos dias, unindo, assim, a comunidade em torno da sua preservação.

Para além disso, haverá que ter presente a necessidade de o regime a estabelecer ser suficientemente flexível para que possa inserir-se nas diversas ordens jurídicas nacionais sem entropias de magnitude tal que ponham em risco os parâmetros essenciais das várias ordens jurídicas ou a viabilidade da harmonização que se procura e que é realmente desejável.

É, pois, caso para dizer, com Francis Bacon, que *em quaisquer coisas difíceis não se deve procurar semear e colher ao mesmo tempo;* é *antes necessária preparação para que elas amadureçam gradualmente*[34].

Lisboa, 15 de Dezembro de 2014

33) Cf. artigo 91.º da proposta de Regulamento.

34) «*In rebus quibuscumque difficilioribus non expectandum, ut quis simul, et serat, et metar, sed praeparatione opus est, ut per gradus maturescant*» - Francis Bacon, *Sermones fideles, sive Interiora Rerum*. Na versão inglesa adaptada pelo próprio autor: «*In all negotiations of difficulty, a man may not look to sow and reap at once; but must prepare business, and so ripen it by degrees*», em *The Works of Francis Bacon*, Baron of Verulam, Viscount Srt. Alban, and Lord High Chancellor of England, Vol. III, Londres, 1740, p. 369.

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


JURIS
PRU
DÊNCIA

ACÓRDÃO
DO TRIBUNAL DE JUSTIÇA
(GRANDE SECÇÃO)

8 de abril de 2014 (*)

«COMUNICAÇÕES ELETRÓNICAS – DIRETIVA 2006/24/CE – SERVIÇOS DE COMUNICAÇÕES ELETRÓNICAS PUBLICAMENTE DISPONÍVEIS OU DE REDES PÚBLICAS DE COMUNICAÇÕES – CONSERVAÇÃO DE DADOS GERADOS OU TRATADOS NO CONTEXTO DA OFERTA DESSES SERVIÇOS – VALIDADE – ARTIGOS 7.°, 8.° E 11.° DA CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA»

Nos processos apensos C293/12 e C594/12, que têm por objeto pedidos de decisão prejudicial apresentados, nos termos do artigo 267.° TFUE, pela High Court (Irlanda) e pelo Verfassungsgerichtshof (Áustria), por decisões, respetivamente, de 27 de janeiro e de 28 de novembro de 2012, que deram entrada no Tribunal de Justiça em 11 junho e 19 de dezembro de 2012, nos processos **Digital Rights Ireland Ltd** (C293/12)

contra **Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlanda, The Attorney General,**

sendo intervenientes: **Irish Human Rights Commission** e **Kärntner Landesregierung** (C594/12), **Michael Seitlinger, Christof Tschohl e o.**,

O TRIBUNAL DE JUSTIÇA (Grande Secção),

composto por: V. Skouris, presidente, K. Lenaerts, vicepresidente, A. Tizzano, R. Silva de Lapuerta, T. von Danwitz (relator), E. Juhász, A. Borg Barthet, C. G. Fernlund e J. L. da Cruz Vilaça, presidentes de secção, A. Rosas, G. Arestis, J.C. Bonichot, A. Arabadjiev, C. Toader e C. Vajda, juízes,

advogado-geral: P. Cruz Villalón,

secretário: K. Malacek, administrador,

vistos os autos e após a audiência de 9 de julho de 2013, vistas as observações apresentadas:

- Em representação da Digital Rights Ireland Ltd, por F. Callanan, SC, e F. Crehan, BL, mandatados por S. McGarr, solicitor,
- Em representação de M. Seitlinger, por G. Otto, Rechtsanwalt,
- Em representação de M. Tschohl e o., por E. Scheucher, Rechtsanwalt,
- Em representação da Irish Human Rights Commission, por P. Dillon Malone, BL, mandatado por S. Lucey, solicitor,
- Em representação da Irlanda, por E. Creedon e D. McGuinness, na qualidade de agentes, assistidos por E. Regan, SC, e D. Fennelly, JC,
- Em representação do Governo austríaco, por G. Hesse e G. Kunnert, na qualidade de agentes,
- Em representação do Governo espanhol, por N. Díaz Abad, na qualidade de agente,
- Em representação do Governo francês, por G. de Bergues, D. Colas e B. BeaupèreManokha, na qualidade de agentes,
- Em representação do Governo italiano, por G. Palmieri, na qualidade de agente, assistida por A. De Stefano, avvocato dello Stato,
- Em representação do Governo polaco, por B. Majczyna e M. Szpunar, na qualidade de agentes,
- Em representação do Governo português, por L. Inez Fernandes e C. Vieira Guerra, na qualidade de agentes,
- Em representação do Governo do Reino Unido, por L. Christie, na qualidade de agente, assistido por S. Lee, barrister,
- Em representação do Parlamento Europeu, por U. Rösslein, A. Caiola e K. Zejdová, na qualidade de agentes,
- Em representação do Conselho da União Europeia, por J. Monteiro, E. Sitbon e I. Šulce, na qualidade de agentes,
- Em representação da Comissão Europeia, por D. Maidani, B. Martenczuk e M. Wilderspin, na qualidade de agentes,
- Ouvidas as conclusões do advogado-geral na audiência de 12 de dezembro de 2013,
- Profere o presente.

ACÓRDÃO

1. Os pedidos de decisão prejudicial têm por objeto a validade da Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE (JO L 105, p. 54).

2. O pedido apresentado pela High Court (processo C-293/12) é relativo a um litígio que opõe a Digital Rights Ireland Ltd. (a seguir «Digital Rights») ao Minister for Communications, Marine and Natural Resources, ao Minister for Justice, Equality and Law Reform, ao Commissioner of the Garda Síochána, à Irlanda e ao Attorney General acerca da legalidade de medidas legislativas e administrativas nacionais respeitantes à conservação de dados relativos a comunicações eletrónicas.

3. O pedido apresentado pelo Verfassungsgerichtshof (processo C-594/12) é relativo a recursos em matéria constitucional interpostos perante este órgão jurisdicional respetivamente pelo Kärntner Landesregierung (Governo do Land de Caríntia), bem como por M. Seitlinger, C. Tschohl e 11 128 outros recorrentes, acerca da compatibilidade da lei que transpõe a Diretiva 2006/24 para o direito interno austríaco com a lei constitucional federal (BundesVerfassungsgesetz).

QUADRO JURÍDICO DIRETIVA 95/46/CE

4. 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 de dados pessoais e à livre circulação desses dados (JO L 281, p. 31), nos termos do seu artigo 1.°, n.° 1, tem por objeto assegurar a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais.

5. Quanto à segurança do tratamento de tais dados, o artigo 17.°, n.° 1, da mesma diretiva dispõe:

   «Os Estados-Membros estabelecerão que o responsável pelo tratamento deve pôr em prática medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a alteração, a difusão ou acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito.

Estas medidas devem assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger».

DIRETIVA 2002/58/CE

6. A Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO L 201, p. 37), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009 (JO L 337, p. 11, a seguir «Diretiva 2002/58»), tem por objeto, de acordo com o seu artigo 1.°, n.° 1, a harmonização das disposições dos Estados-Membros necessárias para garantir um nível equivalente de proteção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade e à confidencialidade, no que respeita ao tratamento de dados pessoais no sector das comunicações eletrónicas, e para garantir a livre circulação desses dados e de equipamentos e serviços de comunicações eletrónicas na Comunidade. Nos termos do n.° 2 do mesmo artigo, as disposições desta diretiva especificam e complementam a Diretiva 95/46/CE para os efeitos enunciados no n.° 1.

7. No que respeita à segurança do tratamento de dados, o artigo 4.° da Diretiva 2002/58 prevê:

   «1. O prestador de um serviço de comunicações eletrónicas publicamente disponível adotará as medidas técnicas e organizativas adequadas para garantir a segurança dos seus serviços, se necessário conjuntamente com o fornecedor da rede pública de comunicações no que respeita à segurança da rede. Tendo em conta o estado da técnica e os custos da sua aplicação, essas medidas asseguram um nível de segurança adequado aos riscos existentes.

   1A Sem prejuízo do disposto na Diretiva 95/46/CE, as medidas referidas no n.° 1 compreendem, no mínimo:

   - a garantia de que aos dados pessoais apenas possa ter acesso pessoal autorizado, para fins autorizados a nível legal,
   - a proteção dos dados pessoais armazenados ou transmitidos contra a destruição acidental ou ilegal, a perda ou alteração acidental e o armazenamento, tratamento, acesso ou divulgação não autorizados ou ilegais, e
   - a garantia da aplicação de uma política de segurança relativa ao tratamento dos dados pessoais.

   As autoridades nacionais competentes devem ter competência para auditar as

medidas tomadas por prestadores de serviços de comunicações eletrónicas acessíveis ao público e para emitir recomendações sobre melhores práticas relativas ao nível de segurança que estas medidas devem alcançar.

2. Em caso de risco especial de violação da segurança da rede, o prestador de um serviço de comunicações eletrónicas publicamente disponível informará os assinantes desse risco e, sempre que o risco se situe fora do âmbito das medidas a tomar pelo prestador do serviço, das soluções possíveis, incluindo uma indicação dos custos prováveis daí decorrentes.»

8. Quanto à confidencialidade das comunicações e dos dados de tráfego, o artigo 5.°, n.os 1 e 3, da referida diretiva dispõe:

«1. Os Estados-Membros garantirão, através da sua legislação nacional, a confidencialidade das comunicações e respetivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações eletrónicas publicamente disponíveis. Proibirão, nomeadamente, a escuta, a instalação de dispositivos de escuta, o armazenamento ou outras formas de interceção ou vigilância de comunicações e dos respetivos dados de tráfego por pessoas que não os utilizadores, sem o consentimento dos utilizadores em causa, exceto quando legalmente autorizados a fazêlo, em conformidade com o disposto no n.° 1 do artigo 15.° O presente número não impede o armazenamento técnico que é necessário para o envio de uma comunicação, sem prejuízo do princípio da confidencialidade.

[...]

3. Os Estados-Membros asseguram que o armazenamento de informações ou a possibilidade de acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador só sejam permitidos se este tiver dado o seu consentimento prévio com base em informações claras e completas, nos termos da Diretiva 95/46/CE, nomeadamente sobre os objetivos do processamento. Tal não impede o armazenamento técnico ou o acesso que tenha como única finalidade efetuar a transmissão de uma comunicação através de uma rede de comunicações eletrónicas, ou que seja estritamente necessário ao fornecedor para fornecer um serviço da sociedade da informação que tenha sido expressamente solicitado pelo assinante ou pelo utilizador.»

9. Nos termos do artigo 6.°, n.° 1, da Diretiva 2002/58:

«Sem prejuízo do disposto nos n.os 2, 3 e 5 do presente artigo e no n.° 1 do artigo 15.°, os dados de tráfego relativos a assinantes e utilizadores tratados e armazenados pelo fornecedor de uma rede pública de comunicações ou de um serviço de comunicações eletrónicas publicamente disponíveis devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação.»

10. O artigo 15.° da Diretiva 2002/58 enuncia, no seu n.° 1:

> «Os Estados-Membros podem adotar medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nos artigos 5.° e 6.°, nos n.os 1 a 4 do artigo 8.° e no artigo 9.° da presente diretiva sempre que essas restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas, tal como referido no n.° 1 do artigo 13.° da Diretiva 95/46/CE. Para o efeito, os Estados-Membros podem designadamente adotar medidas legislativas prevendo que os dados sejam conservados durante um período limitado, pelas razões enunciadas no presente número. Todas as medidas referidas no presente número deverão ser conformes com os princípios gerais do direito comunitário, incluindo os mencionados nos n.os 1 e 2 do artigo 6.o do Tratado da União Europeia.»

DIRETIVA 2006/24

11. Depois de ter efetuado uma consulta aos representantes dos serviços de controlo, do setor das comunicações eletrónicas e dos peritos em matéria de proteção de dados, a Comissão apresentou, em 21 de setembro de 2005, uma avaliação de impacto das opções políticas relativas a regras respeitantes à conservação dos dados de tráfego (a seguir «avaliação de impacto»). Esta avaliação serviu de base à elaboração da proposta de Diretiva do Parlamento Europeu e do Conselho relativa à conservação de dados tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis e que altera a Diretiva 2002/58/CE [COM(2005) 438 final, a seguir «proposta de diretiva»], apresentada na mesma data, que conduziu à adoção da Diretiva 2006/24 ao abrigo do artigo 95.° CE.

12. O considerando 4 da Diretiva 2006/24 enuncia:

> «O n.° 1 do artigo 15.° da Diretiva 2002/58/CE enumera as condições em que os Estados-Membros podem restringir o âmbito dos direitos e obrigações previstos nos artigos 5.° e 6.°, nos n.os 1, 2, 3 e 4 do artigo 8.° e no artigo 9.° da supracitada diretiva. Qualquer restrição deste tipo deve constituir uma medida necessária, adequada e proporcionada numa sociedade democrática, por razões específicas de ordem pública, ou seja, para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública e a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas.»

13. De acordo com a primeira frase do considerando 5 da Diretiva 2006/24, «[v]ários Estados-Membros aprovaram legislação relativa à conservação de dados pelos fornecedores de serviços tendo em vista a prevenção, investigação, deteção e repressão de infrações penais».

14. Os considerandos 7 a 11 da Diretiva 2006/24 têm a seguinte redação:

«(7) Nas suas conclusões, o Conselho 'Justiça e Assuntos Internos' de 19 de dezembro de 2002 assinalou que, devido a um notável crescimento das possibilidades oferecidas pelas comunicações eletrónicas, os dados gerados pela utilização deste tipo de comunicações constituem um instrumento extremamente importante e útil na prevenção, investigação, deteção e de repressão de infrações penais, em especial contra a criminalidade organizada.

(8) Na sua Declaração de 25 de março de 2004 sobre a luta contra o terrorismo, o Conselho Europeu encarregou o Conselho de proceder à análise de propostas relativas ao estabelecimento de regras sobre a conservação de dados de tráfego das comunicações pelos prestadores de serviços.

(9) Nos termos do artigo 8.° da Convenção Europeia dos Direitos do Homem (CEDH) [assinada em Roma em 4 de novembro de 1959], qualquer pessoa tem direito ao respeito da sua vida privada e da sua correspondência. As autoridades públicas só podem interferir no exercício deste direito nos termos previstos na lei e, quando essa ingerência for necessária, numa sociedade democrática, designadamente, para a segurança nacional ou para a segurança pública, a defesa da ordem e a prevenção das infrações penais, ou a proteção dos direitos e das liberdades de terceiros. Visto que a conservação de dados se tem revelado um instrumento de investigação necessário e eficaz de repressão penal em vários Estados-Membros, nomeadamente em matérias tão graves como o crime organizado e o terrorismo, é necessário assegurar que as autoridades responsáveis pela aplicação da lei possam dispor dos dados conservados por um período determinado, nas condições previstas na presente diretiva. […]

(10) Em 13 de julho de 2005, na sua Declaração condenando os ataques terroristas em Londres, o Conselho reafirmou a necessidade de aprovar o mais rapidamente possível medidas comuns relativas à conservação de dados de telecomunicações.

(11) Tendo em consideração a importância dos dados de tráfego e dos dados de localização para a investigação, deteção e repressão de infrações penais, é necessário, como os trabalhos de investigação e a experiência prática em vários Estados-Membros o demonstram, garantir a nível europeu a conservação durante um determinado período dos dados gerados ou tratados, no contexto da oferta de comunicações, pelos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações, nas condições previstas na presente diretiva.»

15. Os considerandos 16, 21 e 22 da referida diretiva especificam:

«(16) As obrigações que incumbem aos fornecedores de serviços, por força do artigo 6.° da Diretiva 95/46/CE, relativamente a medidas destinadas a assegurar a qualidade dos dados, e as obrigações dos mesmos de tomarem medidas para salvaguardar a confidencialidade e a segurança do tratamento de dados por força dos artigos 16.° e 17.° da referida diretiva, são plenamente aplicáveis aos dados conservados em conformidade com a presente diretiva.

(21) Atendendo a que os objetivos da presente diretiva, ou seja, a harmonização das obrigações que incumbem aos fornecedores de conservarem determinados dados e assegurarem que estes sejam disponibilizados para efeitos de investigação, deteção e repressão de crimes graves tal como definidos no direito nacional de cada Estado-Membro, não podem ser suficientemente realizados pelos Estados-Membros e podem, pois, devido à dimensão e aos efeitos da presente diretiva, ser melhor alcançados a nível comunitário, a Comunidade pode tomar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5.° do Tratado. Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, a presente diretiva não excede o necessário para atingir aqueles objetivos.

(22) A presente diretiva respeita os direitos fundamentais e os princípios consagrados nomeadamente na Carta dos Direitos Fundamentais da União Europeia. Em especial, a presente diretiva, conjugada com a Diretiva 2002/58/CE, visa assegurar que sejam plenamente respeitados os direitos fundamentais dos cidadãos em matéria de respeito pela privacidade e pelas comunicações e de proteção dos dados pessoais, consagrados nos artigos 7.° e 8.° da Carta.»

16. A Diretiva 2006/24 consagra a obrigação dos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou das redes públicas de comunicações de conservarem determinados dados por eles gerados ou tratados. A este respeito, os artigos 1.° a 9.°, 11.° e 13.° desta diretiva dispõem:

«*Artigo 1.°* Objeto e âmbito de aplicação

1. A presente diretiva visa harmonizar as disposições dos Estados-Membros relativas às obrigações dos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações em matéria de conservação de determinados dados por eles gerados ou tratados, tendo em vista garantir a disponibilidade desses dados para efeitos de investigação, de deteção e de repressão de crimes graves, tal como definidos no direito nacional de cada Estado Membro.

2. A presente diretiva é aplicável aos dados de tráfego e aos dados de localização relativos quer a pessoas singulares quer a pessoas coletivas, bem como aos

dados conexos necessários para identificar o assinante ou o utilizador registado. A presente diretiva não é aplicável ao conteúdo das comunicações eletrónicas, incluindo as informações consultadas utilizando uma rede de comunicações eletrónicas.

Artigo 2.° Definições

1. Para efeitos da presente diretiva, são aplicáveis as definições constantes da Diretiva 95/46/CE, da Diretiva 2002/21/CE do Parlamento Europeu e do Conselho, de 7 de março de 2002, relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas (diretivaquadro) […], e da Diretiva 2002/58/CE.

2. Para efeitos da presente diretiva, entendese por:

a) 'Dados', os dados de tráfego e os dados de localização, bem como os dados conexos necessários para identificar o assinante ou o utilizador;

b) 'Utilizador', qualquer pessoa singular ou coletiva que utilize um serviço de comunicações eletrónicas publicamente disponível para fins privados ou comerciais, não sendo necessariamente assinante desse serviço;

c) 'Serviço telefónico', os serviços de chamada (incluindo as chamadas vocais, o correio vocal, a teleconferência ou a transmissão de dados), os serviços suplementares (incluindo o reencaminhamento e a transferência de chamadas) e os serviços de mensagens e multimédia [incluindo os serviços de mensagens curtas (SMS), os serviços de mensagens melhorados (EMS) e os serviços multimédia (MMS)];

d) 'Código de identificação de utilizador' (*'user ID'*), um código único atribuído às pessoas, quando estas se tornam assinantes ou se inscrevem num serviço de acesso à internet, ou num serviço de comunicação pela internet;

e) 'Identificador da célula' (*'cell ID'*), a identificação da célula de origem e de destino de uma chamada telefónica numa rede móvel;

f) 'Chamada telefónica falhada', uma comunicação em que a ligação telefónica foi estabelecida, mas que não obteve resposta, ou em que houve uma intervenção do gestor da rede.

Artigo 3.° Obrigação de conservação de dados

1. Em derrogação aos artigos 5.°, 6.° e 9.° da Diretiva 2002/58/CE, os Estados-Membros devem tomar medidas para garantir a conservação, em conformidade com as disposições da presente diretiva, dos dados especificados no artigo 5.° da presente diretiva, na medida em que sejam gerados ou tratados no contexto da oferta dos serviços de comunicações em causa por fornecedores de serviços de

comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações quando estes fornecedores estejam sob a sua jurisdição.

2. A obrigação de conservação de dados impostos no n.° 1 inclui a conservação dos dados especificados no artigo 5.° relativos a chamadas telefónicas falhadas, quando gerados ou tratados, e armazenados (no caso de dados telefónicos) ou registados (no caso de dados da internet) por fornecedores de serviços de comunicações eletrónicas publicamente disponíveis, ou de uma rede pública de comunicações, que estejam sob a jurisdição do Estado-Membro em questão, no contexto da oferta de serviços de comunicação. A presente diretiva não estabelece a conservação de dados relativos a chamadas não estabelecidas.

Artigo 4.° Acesso aos dados

Os Estados-Membros devem tomar medidas para assegurar que os dados conservados em conformidade com a presente diretiva só sejam transmitidos às autoridades nacionais competentes em casos específicos e de acordo com a legislação nacional. Os procedimentos que devem ser seguidos e as condições que devem ser respeitadas para se ter acesso a dados conservados de acordo com os requisitos da necessidade e da proporcionalidade devem ser definidos por cada Estado-Membro no respetivo direito nacional, sob reserva das disposições pertinentes do Direito da União Europeia ou do Direito Internacional Público, nomeadamente a CEDH, na interpretação que lhe é dada pelo Tribunal Europeu dos Direitos do Homem.

Artigo 5.° Categorias de dados a conservar

1. Os Estados-Membros devem assegurar a conservação das categorias de dados seguintes em aplicação da presente diretiva:

a) Dados necessários para encontrar e identificar a fonte de uma comunicação:

1) no que diz respeito às comunicações telefónicas nas redes fixa e móvel:

i) o número de telefone de origem,

ii) o nome e endereço do assinante ou do utilizador registado;

2) no que diz respeito ao acesso à internet, ao correio eletrónico através da internet e às comunicações telefónicas através da internet:

i) o(s) código(s) de identificação atribuído(s) ao utilizador,

ii) o código de identificação do utilizador e o número de telefone atribuídos a qualquer comunicação que entre na rede telefónica pública,

iii) o nome e o endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP, o código de identificação de utilizador, ou o número de telefone estavam atribuídos no momento da comunicação;

b) Dados necessários para encontrar e identificar o destino de uma comunicação:

1) no que diz respeito às comunicações telefónicas nas redes fixa e móvel:

i) o(s) número(s) marcados (o número ou números de telefone de destino) e, em casos que envolvam serviços suplementares, como o reencaminhamento ou a transferência de chamadas, o número ou números para onde a chamada foi reencaminhada,

ii) o nome e o endereço do assinante, ou do utilizador registado;

2) no que diz respeito ao correio eletrónico através da internet e às comunicações telefónicas através da internet:

i) o código de identificação de utilizador ou o número de telefone do destinatário pretendido, ou de uma comunicação telefónica através da internet,

ii) o(s) nome(s) e o(s) endereço(s) do(s) subscritor(es), ou do(s) utilizador(es) registado(s), e o código de identificação de utilizador do destinatário pretendido da comunicação;

c) Dados necessários para identificar a data, a hora e a duração de uma comunicação:

1) no que diz respeito às comunicações telefónicas nas redes fixa e móvel, a data e a hora do início e do fim da comunicação;

2) No que diz respeito ao acesso à internet, ao correio eletrónico através da internet e às comunicações telefónicas através da internet:

i) a data e a hora do início (login) e do fim (logoff) da ligação ao serviço de acesso à internet com base em determinado fuso horário, juntamente com o endereço do protocolo IP, dinâmico ou estático, atribuído pelo fornecedor do serviço de acesso à internet a uma comunicação, bem como o código de identificação de utilizador do subscritor ou do utilizador registado,

ii) a data e a hora do início e do fim da ligação ao serviço de correio eletrónico através da internet ou de comunicações telefónicas através da internet, com base em determinado fuso horário;

d) Dados necessários para identificar o tipo de comunicação:

1) no que diz respeito às comunicações telefónicas nas redes fixa e móvel: o serviço telefónico utilizado;

2) no que diz respeito ao correio eletrónico através da internet e às comunicações telefónicas através da internet: o serviço internet utilizado;

e) Dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento:

1) no que diz respeito às comunicações telefónicas na rede fixa os números de telefone de origem e de destino;

2) no que diz respeito às comunicações telefónicas na rede móvel:

i) os números de telefone de origem e de destino,

ii) a Identidade Internacional de Assinante Móvel ('*International Mobile Subscriber Identity*', ou IMSI) de quem telefona,

iii) a Identidade Internacional do Equipamento Móvel ('*International Mobile Equipment Identity*', ou IMEI) de quem telefona,

iv) a IMSI do destinatário do telefonema,

v) a IMEI do destinatário do telefonema,

vi) no caso dos serviços prépagos de carácter anónimo, a data e a hora da ativação inicial do serviço e o identificador da célula a partir da qual o serviço foi ativado;

3) No que diz respeito ao acesso à internet, ao correio eletrónico através da internet e às comunicações telefónicas através da internet:

i) o número do telefone chamador para acesso por chamada;

ii) a linha de assinante digital ('*digital subscriber line*', ou DSL), ou qualquer outro identificador terminal do autor da comunicação;

f) Dados necessários para identificar a localização do equipamento de comunicação móvel:

1) o identificador da célula no início da comunicação;

2) os dados que identifiquem a situação geográfica das células, tomando como referência os respetivos identificadores de célula durante o período em que se procede à conservação de dados.

2. Nos termos da presente diretiva, não podem ser conservados quaisquer dados que revelem o conteúdo das comunicações.

Artigo 6.° Períodos de conservação

Os Estados-Membros devem assegurar que as categorias de dados referidos no artigo 5.° sejam conservadas por períodos não inferiores a seis meses e não superiores a dois anos, no máximo, a contar da data da comunicação.

Artigo 7.° Proteção e segurança de dados

Sem prejuízo das disposições adotadas nos termos da Diretiva 95/46/CE e da Diretiva 2002/58/CE, cada Estado-Membro deve assegurar que os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações respeitem, no mínimo, os seguintes princípios em matéria de segurança de dados no que se refere aos dados conservados em conformidade com a presente diretiva:

a) Os dados conservados devem ser da mesma qualidade e estar sujeitos à mesma proteção e segurança que os dados na rede;

b) Os dados devem ser objeto de medidas técnicas e organizativas adequadas que os protejam da destruição acidental ou ilícita, da perda ou alteração acidental, ou do armazenamento, tratamento, acesso ou divulgação não autorizado ou ilícito;

c) Os dados devem ser objeto de medidas técnicas e organizativas adequadas para garantir que apenas pessoas especialmente autorizadas tenham acesso aos dados;

d) Os dados devem ser destruídos no final do período de conservação, exceto os dados que tenham sido facultados e preservados.

Artigo 8.° Requisitos para o armazenamento dos dados conservados

Os Estados-Membros devem assegurar que os dados especificados no artigo 5.° sejam conservados em conformidade com a presente diretiva de modo que tais dados e outras informações necessárias relacionadas com esses dados possam ser transmitidos imediatamente, mediante pedido, às autoridades competentes.

Artigo 9.° Autoridade de controlo

1. Cada Estado-Membro deve designar uma ou mais autoridades públicas para controlar a aplicação, no respetivo território, das disposições adotadas pelos Estados-Membros, nos termos do artigo 7.°, no que diz respeito à segurança dos dados conservados. Essas autoridades podem ser as referidas no artigo 28.° da Diretiva 95/46/CE.

2. As autoridades a que se refere o n.° 1 devem atuar com absoluta independência no exercício do controlo da aplicação a que se refere o mesmo número.
[...]

Artigo 11.° Alteração da Diretiva 2002/58/CE

No artigo 15.° da Diretiva 2002/58/CE é inserido o seguinte número:

'1A. O n.° 1 não é aplicável aos dados cuja conservação seja especificamente exigida pela Diretiva 2006/24/CE […] para os fins mencionados no n.° 1 do artigo 1.° dessa diretiva.'
[...]

Artigo 13.° Recursos, responsabilidade e sanções

1. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que as medidas nacionais que dão execução ao capítulo III da Diretiva 95/46/CE relativo a recursos judiciais, responsabilidade e sanções sejam plenamente aplicadas no que se refere ao tratamento de dados no âmbito da presente diretiva.

2.Os Estados-Membros devem tomar, em particular, as medidas necessárias para assegurar que o acesso ou a transferência intencional de dados conservados em conformidade com a presente diretiva, não permitido pelo direito nacional adotado em virtude da presente diretiva, seja punível por sanções, incluindo sanções administrativas ou penais, que sejam efetivas, proporcionadas e dissuasivas.»

LITÍGIOS NO PROCESSO PRINCIPAL E QUESTÕES PREJUDICIAIS
PROCESSO C-293/12

17. A Digital Rights interpôs, em 11 de agosto de 2006, um recurso na High Court, no qual alega que é proprietária de um telefone móvel, registado em 3 de junho de 2006, que utiliza desde essa data. Põe em causa a legalidade de medidas legislativas e administrativas nacionais respeitantes à conservação de dados relativos a comunicações eletrónicas e pede, designadamente, ao órgão jurisdicional de reenvio que declare a nulidade da Diretiva 2006/24 e da sétima parte da lei de 2005 sobre Justiça Penal (infrações terroristas) [Criminal Justice (Terrorist Offences) Act 2005] que prevê que os fornecedores de serviços de comunicações telefónicas devem conservar os dados respeitantes a estas últimas relativos ao tráfego e à localização durante um período determinado por lei, com objetivos de prevenção e deteção das infrações, de investigação e repressão das mesmas, e para garantir a segurança do Estado.

18. A High Court, considerando que não pode dirimir as questões relativas ao direito nacional que lhe foram submetidas sem que a validade da Diretiva 2006/24 tenha sido apreciada, decidiu suspender a instância e submeter ao Tribunal de Justiça as seguintes questões prejudiciais:

«1) A restrição dos direitos da [recorrente], no que respeita à utilização da rede telefónica móvel, resultante das exigências dos artigos 3.°, 4.° e 6.° da Diretiva 2006/24/CE é incompatível com o artigo 5.°, n.° 4, TUE, na medida em que é desproporcionada e desnecessária ou inadequada para alcançar os objetivos legítimos de:

a) assegurar que determinados dados são disponibilizados para efeitos de investigação, deteção e repressão de crimes graves?

e/ou

b) assegurar o funcionamento adequado do mercado interno da União Europeia?

2) Concretamente,

a) A Diretiva 2006/24/CE é compatível com o direito dos cidadãos de circularem e permanecerem livremente no território dos Estados-Membros, consagrado no artigo 21.° TFUE?

b) A Diretiva 2006/24/CE é compatível com o direito ao respeito pela vida privada, consagrado no artigo 7.° da Carta [dos Direitos Fundamentais da União Europeia (a seguir 'Carta')] e no artigo 8.° da [CEDH]?

c) A Diretiva 2006/24/CE é compatível com o direito à proteção dos dados pessoais, consagrado no artigo 8.° da Carta?

d) A Diretiva 2006/24/CE é compatível com o direito à liberdade de expressão, consagrado no artigo 11.° da Carta e no artigo 10.° da CEDH?

e) A Diretiva 2006/24/CE é compatível com o direito a uma boa administração, consagrado no artigo 41.° da Carta?

3)Em que medida os Tratados e, em concreto, o princípio da cooperação leal previsto no artigo 4.°, n.° 3, TUE, exigem que os tribunais investiguem e apreciem a compatibilidade das medidas nacionais de transposição da Diretiva 2006/24/CE com as garantias conferidas pela Carta, incluindo o seu artigo 7.° (cujo conteúdo é inspirado no artigo 8.° da CEDH)?»

PROCESSO C-594/12

19. Na origem do pedido de decisão prejudicial no processo C-594/12 estão vários recursos interpostos no Verfassungsgerichtshof, respetivamente pela Kärntner Landesregierung e por M. Seitlinger, C. Tschohl e 11 128 outros recorrentes que pedem a anulação do artigo 102.°A da Lei de 2003 sobre as telecomunicações (Telekommunikationsgesetz 2003), introduzido nesta lei pela lei de alteração (Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird, BGBl. I, 27/2011) para efeitos da transposição da Diretiva 2006/24 para o direito interno austríaco. Estas partes consideram, designadamente, que este artigo 102.°A viola o direito fundamental dos particulares à proteção dos seus dados.

20. O Verfassungsgerichtshof perguntase, designadamente, se a Diretiva 2006/24 é compatível com a Carta na medida em que permite o armazenamento de um volume de tipos de dados relativos a um número ilimitado de pessoas durante um

longo período. A conservação dos dados abrange quase exclusivamente pessoas cujo comportamento não justifica, de modo nenhum, que os seus dados sejam conservados. Estas pessoas ficam expostas a um risco superior de que as autoridades investiguem os seus dados, tomem conhecimento do seu conteúdo, se informem acerca da sua vida privada e utilizem estes dados com múltiplas finalidades, tendo designadamente em conta o número incomensurável de pessoas que têm acesso aos dados durante um período de, pelo menos, seis meses. Segundo o órgão jurisdicional de reenvio, existem dúvidas, por um lado, quanto ao facto de esta diretiva poder alcançar os objetivos que prossegue e, por outro, quanto ao caráter proporcionado da ingerência nos direitos fundamentais em causa.

21. Nestas condições, o Verfassungsgerichtshof decidiu suspender a instância e submeter ao Tribunal de Justiça as seguintes questões prejudiciais:

«1) Quanto à validade dos atos adotados pelas instituições da União:

Os artigos 3.° a 9.° da Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE, são compatíveis com os artigos 7.°, 8.° e 11.° da [Carta]?

2) Quanto à interpretação dos Tratados:

a) À luz das anotações ao artigo 8.° da Carta, as quais, nos termos do artigo 52.°, n.° 7, da Carta, devem ser tidas em devida conta pelo Verfassungsgerichtshof como orientações para a interpretação da referida Carta, 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 de dados pessoais e à livre circulação desses dados e o Regulamento (CE) n.° 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados [(JO 2001, L 8, p. 1)], devem ser tidos em consideração de forma equivalente às condições constantes do artigo 8.°, n.° 2, e do artigo 52.°, n.° 1, da Carta, ao apreciar a admissibilidade das ingerências?

b) Qual é a relação existente entre o 'direito da União' referido na última frase do artigo 52.°, n.° 3, da Carta, e as diretivas em matéria do direito à proteção de dados?

c) Atendendo ao facto de a Diretiva 95/46/CE e o Regulamento (CE) n.° 45/2001 imporem condições e restrições na salvaguarda do direito fundamental à proteção de dados constante da Carta, as alterações resultantes

do direito derivado posterior devem ser tidas em consideração ao interpretar o artigo 8.° da Carta?

d) Considerando o artigo 52.°, n.° 4, da Carta, resulta do princípio da salvaguarda de um nível de proteção mais elevado, consagrado no artigo 53.° da Carta, que os limites, estabelecidos pela Carta, para as restrições que podem ser colocadas pelo direito derivado devem ser definidos de acordo com critérios mais exigentes?

e) Considerando o artigo 52.°, n.° 3, da Carta, o artigo 5.° do preâmbulo e as anotações ao artigo 7.° da Carta, nos termos das quais os direitos aí garantidos correspondem aos direitos garantidos pelo artigo 8.° da CEDH, é possível deduzir da jurisprudência do Tribunal Europeu dos Direitos do Homem em relação ao artigo 8.° da CEDH a existência de elementos de interpretação do artigo 8.° da Carta que possam influenciar a interpretação deste último artigo?»

22. Por decisão do presidente do Tribunal de Justiça de 11 de junho de 2013, os processos C-293/12 e C-594/12 foram apensados para efeitos da fase oral e do acórdão.

QUANTO ÀS QUESTÕES PREJUDICIAIS

QUANTO À SEGUNDA QUESTÃO, ALÍNEAS B) A D), NO PROCESSO C-293/12, E À PRIMEIRA QUESTÃO NO PROCESSO C-594/12

23. Com a segunda questão, alíneas b) a d), no processo C-293/12, e com a primeira questão no processo C-594/12, que devem ser analisadas conjuntamente, os órgãos jurisdicionais de reenvio pedem, em substância, ao Tribunal de Justiça que aprecie a validade da Diretiva 2006/24 à luz dos artigos 7.°, 8.° e 11.° da Carta.

Quanto à pertinência dos artigos 7.°, 8.° e 11.° da Carta no que respeita à questão da validade da Diretiva 2006/24.

24. Resulta do artigo 1.°, bem como dos considerandos 4, 5, 7 a 11, 21 e 22 da Diretiva 2006/24 que esta visa harmonizar as disposições dos Estados-Membros relativas à conservação, pelos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou das redes públicas de comunicações, de determinados dados por eles gerados ou tratados, tendo em vista garantir a disponibilidade desses dados para efeitos de investigação, de deteção e de repressão de infrações graves, como os associados ao crime organizado e ao terrorismo, no respeito dos direitos consagrados nos artigos 7.° e 8.° da Carta.

25. A obrigação dos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou das redes públicas de comunicações, prevista no artigo 3.° da Diretiva 2006/24, de conservarem os dados enumerados no artigo 5.° da mesma para, se necessário, os disponibilizarem às autoridades nacionais competentes suscita questões relativas à proteção tanto da vida privada como das comunicações consagrada no artigo 7.° da Carta, à proteção de dados pessoais prevista no artigo 8.° da mesma, assim como ao respeito da liberdade de expressão garantida pelo artigo 11.° da Carta.

26. A este respeito, importa salientar que os dados que os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou das redes públicas de comunicações devem conservar, nos termos dos artigos 3.° e 5.° da Diretiva 2006/24, são, designadamente, os dados necessários para encontrar e identificar a fonte e o destino de uma comunicação, para determinar a data, a hora, a duração e o tipo de uma comunicação, o equipamento de comunicação dos utilizadores, bem como para localizar o equipamento de comunicação móvel, dados entre os quais figuram, designadamente, o nome e o endereço do assinante ou do utilizador registado, o número de telefone de origem e o número do destinatário, bem como um endereço IP para os serviços Internet. Estes dados permitem, designadamente, saber qual é a pessoa com quem um assinante ou um utilizador registado comunicou e através de que meio, assim como determinar o tempo da comunicação e o local a partir do qual esta foi efetuada. Além disso, permitem conhecer a frequência das comunicações do assinante ou do utilizador registado com certas pessoas durante um determinado período.

27. Estes dados, considerados no seu todo, são suscetíveis de permitir tirar conclusões muito precisas relativamente à vida privada das pessoas cujos dados foram conservados, como os hábitos da vida quotidiana, os locais em que se encontram de forma permanente ou temporária, as deslocações diárias ou outras, as atividades exercidas, as relações sociais e os meios sociais frequentados.

28. Em tais circunstâncias, apesar de a Diretiva 2006/24 não autorizar, como resulta dos seus artigos 1.°, n.° 2, e 5.°, n.° 2, a conservação do conteúdo da comunicação e das informações consultadas utilizando uma rede de comunicações eletrónicas, não está excluído que a conservação dos dados em causa possa ter incidência sobre a utilização, pelos assinantes ou pelos utilizadores registados, dos meios de comunicação abrangidos por esta diretiva e, consequentemente, sobre o exercício, por estes últimos, da sua liberdade de expressão, garantida pelo artigo 11.° da Carta.

29. A conservação dos dados para efeitos do eventual acesso aos mesmos pelas autoridades nacionais competentes, como prevista pela Diretiva 2006/24, diz direta e especificamente respeito à vida privada e, assim, aos direitos garantidos pelo artigo 7.° da Carta. Além disso, essa conservação dos dados está abrangida

pelo âmbito de aplicação do artigo 8.° desta dado que constitui um tratamento de dados pessoais na aceção deste artigo e deve, assim, necessariamente respeitar as exigências de proteção de dados resultantes deste artigo (acórdão Volker und Markus Schecke e Eifert, C-92/09 e C-93/09, EU:C:2010:662, n.° 47).

30. Embora suscitem designadamente a questão de princípio de saber se os dados dos assinantes e dos utilizadores registados, à luz do artigo 7.° da Carta, podem ou não ser conservados, os reenvios prejudiciais nos presentes processos colocam igualmente a questão de saber se a Diretiva 2006/24 respeita as exigências de proteção dos dados pessoais resultantes do artigo 8.° da Carta.

31. À luz das considerações precedentes, para responder à segunda questão, alíneas b) a d), no processo C-293/12, e à primeira questão no processo C-594/12, importa analisar a validade da Diretiva 2006/24 à luz dos artigos 7.° e 8.° da Carta.

QUANTO À EXISTÊNCIA DE UMA INGERÊNCIA NOS DIREITOS CONSAGRADOS PELOS ARTIGOS 7.° E 8.° DA CARTA

32. Ao impor a conservação dos dados enumerados no artigo 5.°, n.° 1, da Diretiva 2006/24 e ao permitir o acesso das autoridades nacionais competentes aos mesmos, esta diretiva derroga, como salientou o advogadogeral designadamente nos n.os 39 e 40 das suas conclusões, o regime de proteção do direito ao respeito da vida privada, instituído pelas Diretivas 95/46 e 2002/58, em relação ao tratamento de dados pessoais no setor das comunicações eletrónicas, dado que estas diretivas consagram a confidencialidade das comunicações e dos dados relativos ao tráfego, bem como a obrigação de eliminar ou de tornar anónimos esses dados quando deixam de ser necessários para a transmissão de uma comunicação, salvo se forem necessários para a faturação e unicamente enquanto esta necessidade persistir.

33. Para demonstrar a existência de uma ingerência no direito fundamental ao respeito da vida privada, pouco importa que as informações relativas à vida privada em questão tenham ou não caráter sensível ou que os interessados tenham ou não sofrido eventuais inconvenientes em razão dessa ingerência (v., neste sentido, acórdão Österreichischer Rundfunk e o., C-465/00, C-138/01 e C-139/01, EU:C:2003:294, n.° 75).

34. Daí resulta que a obrigação imposta pelos artigos 3.° e 6.° da Diretiva 2006/24 aos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou das redes públicas de comunicações de conservarem durante um determinado período dados relativos à vida privada de uma pessoa e às suas

comunicações, como os previstos no artigo 5.° desta diretiva, constitui em si mesma uma ingerência nos direitos garantidos pelo artigo 7.° da Carta.

35. Além disso, o acesso das autoridades nacionais competentes aos dados constitui uma ingerência suplementar neste direito fundamental (v., no que respeita ao artigo 8.° da CEDH, acórdãos Tribunal EDH, Leander c. Suécia, 26 de março de 1987, série A n°116, § 48; Rotaru c. Roménia [GC], n.° 28341/95, § 46, CEDH 2000V, e Weber e Saravia c. Alemanha (dec.), n.° 54934/00, § 79, CEDH 2006XI). Assim, os artigos 4.° e 8.° da Diretiva 2006/24, que estabelecem regras relativas ao acesso das autoridades nacionais competentes aos dados, são igualmente constitutivos de uma ingerência nos direitos garantidos pelo artigo 7.° da Carta.

36. Do mesmo modo, a Diretiva 2006/24 é constitutiva de uma ingerência no direito fundamental à proteção dos dados pessoais garantido pelo artigo 8.° da Carta, dado que prevê um tratamento dos dados pessoais.

37. Há que constatar que a ingerência que a Diretiva 2006/24 comporta nos direitos fundamentais consagrados nos artigos 7.° e 8.° da Carta, como também salientou o advogadogeral, entre outros, nos n.os 77 e 80 das suas conclusões, é de grande amplitude e deve ser considerada particularmente grave. Além disso, o facto de a conservação e a utilização posterior dos dados serem efetuadas sem que o assinante ou o utilizador registado disso sejam informados é suscetível de gerar no espírito das pessoas abrangidas, como salientou o advogadogeral nos n.os 52 e 72 das suas conclusões, o sentimento de que a sua vida privada é objeto de vigilância constante.

QUANTO À JUSTIFICAÇÃO DA INGERÊNCIA NOS DIREITOS GARANTIDOS PELOS ARTIGOS 7.° E 8.° DA CARTA

38. Em conformidade com o artigo 52.°, n.° 1, da Carta, quaisquer restrições ao exercício dos direitos e liberdades reconhecidos por esta devem ser previstas por lei, respeitar o conteúdo essencial desses direitos e liberdades e, na observância do princípio da proporcionalidade, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros.

39. No que respeita ao conteúdo essencial do direito fundamental ao respeito da vida privada e dos outros direitos consagrados no artigo 7.° da Carta, deve observarse que, embora a conservação dos dados imposta pela Diretiva 2006/24 constitua uma ingerência particularmente grave nestes direitos, não é suscetível de afetar o referido conteúdo tendo em conta que, como resulta do seu artigo 1.°, n.° 2, esta diretiva não permite tomar conhecimento do conteúdo das comunicações eletrónicas enquanto tal.

40. Esta conservação dos dados também não é suscetível de afetar o conteúdo essencial do direito fundamental à proteção dos dados pessoais, consagrado no artigo 8.° da Carta, dado que a Diretiva 2006/24 prevê, no seu artigo 7.°, uma regra relativa à proteção e à segurança dos dados segundo a qual, sem prejuízo das disposições adotadas nos termos das Diretivas 95/46 e 2002/58, devem ser respeitados certos princípios de proteção e de segurança dos dados pelos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, princípios de acordo com os quais os Estados-Membros devem assegurar a adoção de medidas técnicas e organizacionais adequadas contra a destruição acidental ou ilícita, a perda ou a alteração acidental dos dados.

41. Quanto à questão de saber se a referida ingerência corresponde a um objetivo de interesse geral, importa salientar que, se a Diretiva 2006/24 visa harmonizar as disposições dos Estados-Membros relativas às obrigações dos referidos fornecedores em matéria de conservação de determinados dados por eles gerados ou tratados, o objetivo material desta diretiva, como resulta do seu artigo 1.°, n.° 1, consiste em garantir a disponibilidade desses dados para efeitos de investigação, de deteção e de repressão de infrações graves, tal como definidas no direito interno de cada Estado-Membro. O objetivo material desta diretiva é pois contribuir para a luta contra a criminalidade grave e assim, em última análise, para a segurança pública.

42. Resulta da jurisprudência do Tribunal de Justiça que a luta contra o terrorismo constitui um objetivo de interesse geral da União com vista à manutenção da paz e da segurança internacionais (v., neste sentido, acórdãos Kadi e Al Barakaat International Foundation/Conselho e Comissão, C-402/05 P e C-415/05 P, EU:C:2008:461, n.° 363, e AlAqsa/Conselho, C-539/10 P e C-550/10 P, EU:C:2012:711, n.° 130). O mesmo acontece com a luta contra a criminalidade grave com o objetivo de garantir a segurança pública (v., neste sentido, acórdão Tsakouridis, C145/09, EU:C:2010:708, n.os 46 e 47). Além disso, importa salientar, a este respeito, que o artigo 6.° da Carta consagra o direito das pessoas não só à liberdade mas também à segurança.

43. A este respeito, resulta do considerando 7 da Diretiva 2006/24 que, devido a um notável crescimento das possibilidades oferecidas pelas comunicações eletrónicas, o Conselho «Justiça e Assuntos Internos» de 19 de dezembro de 2002 considerou que os dados gerados pela utilização dessas comunicações são particularmente importantes e constituem, portanto, um instrumento útil na prevenção de infrações e na luta contra a criminalidade, designadamente a criminalidade organizada.

44. Impõe-se pois observar que a conservação dos dados com vista a permitir o eventual acesso aos mesmos pelas autoridades nacionais competentes, tal como imposta pela Diretiva 2006/24, corresponde efetivamente a um objetivo de interesse geral.

45. Nestas condições, há que analisar a proporcionalidade da ingerência observada.

46. A este propósito, cabe recordar que o princípio da proporcionalidade exige, segundo jurisprudência constante do Tribunal de Justiça, que os atos das instituições da União sejam adequados para a realização dos objetivos legítimos prosseguidos pela regulamentação em causa e não excedam os limites do que é adequado e necessário para a realização desses objetivos (v., neste sentido, acórdãos Afton Chemical, C-343/09, EU:C:2010:419, n.° 45; Volker und Markus Schecke e Eifert, EU:C:2010:662, n.° 74; Nelson e o., C-581/10 e C-629/10, EU:C:2012:657, n.° 71; Sky Österreich, C-283/11, EU:C:2013:28, n.° 50, e Schaible, C-101/12, EU:C:2013:661, n.° 29).

47. No que respeita à fiscalização jurisdicional do respeito destes requisitos, uma vez que estão em causa ingerências em direitos fundamentais, o alcance do poder de apreciação do legislador da União pode revelarse limitado em função de um certo número de elementos, entre os quais figuram, designadamente, o domínio em questão, a natureza do direito em causa garantido pela Carta, a natureza e a gravidade da ingerência, bem como a finalidade da mesma (v., por analogia, no que respeita ao artigo 8.° da CEDH, acórdão Tribunal EDH, S e Marper c. Reino Unido [GC], n^{os} 30562/04 e 30566/04, § 102, CEDH 2008V).

48. No caso vertente, tendo em conta, por um lado, o importante papel desempenhado pela proteção dos dados pessoais na perspetiva do direito fundamental ao respeito pela vida privada e, por outro, a amplitude e a gravidade da ingerência neste direito que a Diretiva 2006/24 comporta, o poder de apreciação do legislador da União é reduzido, havendo que proceder a uma fiscalização estrita.

49. No que respeita à questão de saber se a conservação dos dados é adequada para a realização do objetivo prosseguido pela Diretiva 2006/24, cumpre observar que, tendo em conta a importância crescente dos meios de comunicação eletrónica, os dados que devem ser conservados em aplicação desta diretiva permitem às autoridades nacionais competentes em matéria penal dispor de possibilidades suplementares de elucidação das infrações graves e, portanto, nesta perspetiva, constituem um instrumento útil para as investigações penais. Assim, a conservação desses dados pode ser considerada adequada à realização do objetivo prosseguido pela referida diretiva.

50. Esta apreciação não é posta em causa pela circunstância, invocada designadamente por C. Tschohl e M. Seitlinger, bem como pelo Governo português nas observações escritas que apresentou ao Tribunal de Justiça, de existirem diversas modalidades de comunicações eletrónicas que não estão abrangidas pelo âmbito de aplicação da Diretiva 2006/24 ou que permitem uma comunicação anónima. Embora seja verdade que esta circunstância é suscetível de limitar a adequação da medida de conservação

dos dados para a realização do objetivo prosseguido, não é, todavia, suscetível de a tornar inapta, como salientou o advogadogeral no n.° 137 das suas conclusões.

51. No que respeita ao caráter necessário da conservação dos dados imposta pela Diretiva 2006/24, cabe observar que é verdade que a luta contra a criminalidade grave, designadamente a criminalidade organizada e o terrorismo, assume primordial importância para garantir a segurança pública e a sua eficácia pode depender em larga medida da utilização das técnicas modernas de investigação. No entanto, tal objetivo de interesse geral, por mais fundamental que seja, não pode, por si só, justificar que uma medida de conservação como a que foi instituída pela Diretiva 2006/24 seja considerada necessária para efeitos da referida luta.

52. Quanto ao direito ao respeito pela vida privada, em conformidade com jurisprudência constante do Tribunal de Justiça, a proteção deste direito fundamental exige, em quaisquer circunstâncias, que as derrogações à proteção dos dados pessoais e as suas limitações devem ocorrer na estrita medida do necessário (acórdão IPI, C-473/12, EU:C:2013:715, n.° 39 e jurisprudência referida).

53. A este respeito, cabe recordar que a proteção dos dados pessoais, que resulta da obrigação expressa prevista no artigo 8.°, n.° 1, da Carta, assume particular importância para o direito ao respeito da vida privada consagrado no artigo 7.° desta.

54. Assim, a regulamentação da União em causa deve estabelecer regras claras e precisas que regulem o âmbito e a aplicação da medida em causa e imponham exigências mínimas, de modo que as pessoas cujos dados foram conservados disponham de garantias suficientes que permitam proteger eficazmente os seus dados pessoais contra os riscos de abuso e contra qualquer acesso e utilização ilícita dos mesmos (v., por analogia, no que respeita ao artigo 8.° da CEDH, acórdãos do Tribunal EDH, Liberty e outros c. Reino Unido, n.° 58243/00, § 62 e 63, de 1 de julho de 2008; Rotaru c. Roménia, já referido, § 57 a 59, e S e Marper c. Reino Unido, já referido, § 99).

55. A necessidade de dispor de tais garantias é ainda mais importante quando, como prevê a Diretiva 2006/24, os dados pessoais são objeto de tratamento automático e existe um risco significativo de acesso ilícito aos mesmos (v., por analogia, no que respeita ao artigo 8.° da CEDH, acórdãos do Tribunal EDH, S e Marper c. Reino Unido, já referido, § 103, e M. K. c. França, n.° 19522/09, § 35, de 18 de abril de 2013).

56. Quanto à questão de saber se a ingerência que a Diretiva 2006/24 comporta se limita ao estritamente necessário, importa salientar que esta diretiva impõe, nos termos do seu artigo 3.°, conjugado com o seu artigo 5.°, n.° 1, a conservação de todos os dados relativos ao tráfego respeitante à rede telefónica fixa, à rede telefónica móvel, ao acesso à Internet, ao correio eletrónico através da Internet e às comunicações telefónicas

através da Internet. Assim, visa todos os meios de comunicação eletrónica cuja utilização está muito generalizada e é de importância crescente na vida quotidiana de todos. Além disso, em conformidade com o seu artigo 3.°, a referida diretiva abrange todos os assinantes e utilizadores registados. Comporta, portanto, uma ingerência nos direitos fundamentais de quase toda a população europeia.

57. A este propósito, importa observar, em primeiro lugar, que a Diretiva 2006/24 abrange de forma generalizada todas as pessoas, todos os meios de comunicação eletrónica e todos os dados relativos ao tráfego, não sendo efetuada uma diferenciação, limitação ou exceção em função do objetivo de luta contra as infrações graves.

58. Com efeito, por um lado, a Diretiva 2006/24 abrange, em geral, todas as pessoas que utilizam serviços de comunicações eletrónicas, sem que, no entanto, as pessoas cujos dados são conservados se encontrem, mesmo indiretamente, numa situação suscetível de dar lugar a ações penais. Assim, aplicase mesmo a pessoas para as quais não existe nenhum indício suscetível de fazer crer que o seu comportamento possa ter uma qualquer relação, mesmo indireta ou longínqua, com infrações graves. Além disso, não prevê nenhuma exceção, pelo que é aplicável mesmo a pessoas cujas comunicações, segundo as regras do direito nacional, estão sujeitas ao segredo profissional.

59. Por outro lado, embora tenha por objetivo contribuir para a luta contra a criminalidade grave, a referida diretiva não exige nenhuma relação entre os dados cuja conservação está prevista e uma ameaça para a segurança pública e, designadamente, não se limita a uma conservação que abranja dados relativos a um período temporal e/ou a uma zona geográfica determinada e/ou a um círculo de pessoas determinadas que possam estar associadas, de uma maneira ou de outra, a uma infração grave, ou a pessoas cuja conservação dos dados pudesse, por outros motivos, contribuir para a prevenção, a deteção ou a repressão de infrações graves.

60. Em segundo lugar, a esta ausência geral de limites acresce que a Diretiva 2006/24 não estabelece um critério objetivo que permita delimitar o acesso das autoridades nacionais competentes aos dados e a sua utilização posterior para prevenir, detetar ou agir penalmente contra infrações suscetíveis de ser consideradas, à luz da amplitude e da gravidade da ingerência nos direitos fundamentais consagrados nos artigos 7.° e 8.° da Carta, suficientemente graves para justificar tal ingerência. Pelo contrário, a Diretiva 2006/24 limitase a remeter, no seu artigo 1.°, n.° 1, de forma genérica, para os crimes graves tal como definidos no direito nacional cada Estado-Membro.

61. Além disso, quanto ao acesso das autoridades nacionais competentes aos dados e à sua utilização posterior, a Diretiva 2006/24 não contém as correspondentes condições materiais e processuais. O artigo 4.° desta diretiva, que regula o acesso destas autoridades aos dados conservados, não dispõe expressamente que este

acesso e a utilização posterior dos dados em causa devem limitarse estritamente a fins de prevenção e de deteção de infrações graves delimitadas com precisão ou a ações penais contra as mesmas, limitandose a dispor que cada Estado-Membro define os procedimentos que devem ser seguidos e as condições que devem ser respeitadas para se ter acesso a dados conservados de acordo com os requisitos da necessidade e da proporcionalidade.

62. Em particular, a Diretiva 2006/24 não estabelece um critério objetivo que permita limitar o número de pessoas com autorização de acesso e de utilização posterior dos dados conservados ao estritamente necessário à luz do objetivo prosseguido. O acesso aos dados conservados pelas autoridades nacionais competentes não está sobretudo sujeito a um controlo prévio efetuado por um órgão jurisdicional ou por uma entidade administrativa independente cuja decisão vise limitar o acesso aos dados e a utilização dos mesmos ao estritamente necessário para alcançar o objetivo prosseguido e ocorra na sequência de um pedido fundamentado destas autoridades apresentado no âmbito de procedimentos de prevenção, deteção ou ação penal. Também não foi prevista uma obrigação precisa de os Estados-Membros estabelecerem tais limitações.

63. Em terceiro lugar, no que respeita à duração da conservação dos dados, a Diretiva 2006/24 impõe, no seu artigo 6.°, que os mesmos sejam conservados por períodos não inferiores a seis meses, não procedendo a uma distinção entre as categorias de dados previstas no artigo 5.° desta diretiva em função da eventual utilidade dos dados relativamente ao objetivo prosseguido ou em função das pessoas em causa.

64. Além disso, a referida duração situase entre um mínimo de seis meses e um máximo de vinte e quatro meses, sem que se especifique que a determinação do período de conservação deve basearse em critérios objetivos a fim de garantir que se limita ao estritamente necessário.

65. Resulta do que precede que a Diretiva 2006/24 não estabelece regras claras e precisas que regulem o alcance da ingerência nos direitos fundamentais consagrados nos artigos 7.° e 8.° da Carta. Impõese pois concluir que esta diretiva comporta uma ingerência nestes direitos fundamentais de grande amplitude e particular gravidade na ordem jurídica da União, sem que essa ingerência seja enquadrada com precisão por disposições que permitam garantir que a mesma se limita efetivamente ao estritamente necessário.

66. Acresce que, no que respeita às regras relativas à segurança e à proteção dos dados conservados pelos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, há que concluir que a Diretiva 2006/24 não prevê garantias suficientes, como exige o artigo 8.° da

Carta, que permitam assegurar uma proteção eficaz dos dados conservados contra os riscos de abuso bem como contra qualquer utilização ilícita dos mesmos. Com efeito, em primeiro lugar, o artigo 7.° da Diretiva 2006/24 não estabelece regras específicas e adaptadas à grande quantidade de dados cuja conservação é imposta por esta diretiva, ao caráter sensível destes dados e ao risco de acesso ilícito aos mesmos, regras que se destinariam designadamente a regular de maneira clara e estrita a proteção e a segurança dos dados em causa, a fim de garantir a sua plena integridade e confidencialidade. Além disso, também não foi prevista uma obrigação precisa de os Estados-Membros estabelecerem tais regras.

67. O artigo 7.° da Diretiva 2006/24, conjugado com os artigos 4.°, n.° 1, da Diretiva 2002/58 e 17.°, n.° 1, segundo parágrafo, da Diretiva 95/46, não garante que seja aplicado pelos referidos fornecedores um nível particularmente elevado de proteção e de segurança através de medidas técnicas e organizacionais, mas autoriza designadamente estes fornecedores, ao determinarem o nível de segurança que aplicam, a terem em conta considerações económicas no que respeita aos custos de aplicação das medidas de segurança. Em especial, a Diretiva 2006/24 não garante a destruição definitiva dos dados no termo do período de conservação dos mesmos.

68. Em segundo lugar, deve acrescentarse que a referida diretiva não impõe que os dados em causa sejam conservados no território da União, pelo que não se pode considerar que esteja plenamente garantida a fiscalização, por uma entidade independente, expressamente exigida pelo artigo 8.°, n.° 3, da Carta, do cumprimento das exigências de proteção e de segurança, tal como referidas nos dois números anteriores. Ora, semelhante fiscalização, efetuada com base no direito da União, constitui um elemento essencial do respeito da proteção das pessoas relativamente ao tratamento dos dados pessoais (v., neste sentido, acórdão Comissão/Áustria, C-614/10, EU:C:2012:631, n.° 37).

69. À luz de todas as considerações precedentes, há que considerar que, ao adotar a Diretiva 2006/24, o legislador da União excedeu os limites impostos pelo respeito do princípio da proporcionalidade à luz dos artigos 7.°, 8.° e 52.°, n.° 1, da Carta.

70. Nestas condições, não há que apreciar a validade da Diretiva 2006/24 à luz do artigo 11.° da Carta.

71. Por conseguinte, há que responder à segunda questão, alíneas b) a d), no processo C-293/12 e à primeira questão no processo C-594/12 que a Diretiva 2006/24 é inválida.

QUANTO À PRIMEIRA QUESTÃO, À SEGUNDA QUESTÃO, ALÍNEAS A) E E), E À TERCEIRA QUESTÃO NO PROCESSO C-293/12, E QUANTO À SEGUNDA QUESTÃO NO PROCESSO C-594/12

72. Resulta do que foi decidido no número anterior que não há que responder à primeira questão, à segunda questão, alíneas a) e e), e à terceira questão no processo C-293/12 nem à segunda questão no processo C-594/12.

QUANTO ÀS DESPESAS

73. Revestindo o processo, quanto às partes na causa principal, a natureza de incidente suscitado perante o órgão jurisdicional de reenvio, compete a este decidir quanto às despesas. As despesas efetuadas pelas outras partes para a apresentação de observações ao Tribunal de Justiça não são reembolsáveis.

Pelos fundamentos expostos, o Tribunal de Justiça (Grande Secção) declara:

A Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE, é inválida.

Assinaturas

* Línguas do processo: inglês e alemão.

ANOTAÇÃO

Neste acórdão o Tribunal de Justiça da União Europeia (TJUE) declara a invalidade da Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, que altera a Diretiva 2002/58/CE. A declaração de invalidade tem por fundamento a violação do princípio da proporcionalidade na restrição que a Diretiva opera dos direitos ao respeito pela vida privada e familiar e à proteção de dados pessoais, consagrados nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia (UE).

A declaração de invalidade da Diretiva não implica diretamente a invalidade da lei nacional que a transponha, mas é imperativo avaliar a conformidade desta com o Direito da União Europeia, em especial com a Carta dos Direitos Fundamentais da UE.

A Diretiva 2006/24/CE caracterizava-se por ser uma diretiva derrogatória, na medida em que era um ato normativo exclusivamente restritivo dos direitos consagrados nos artigos 7.º e 8.º da Carta, derrogando para o efeito os artigos 5.º, 6.º e 9.º da Diretiva 2002/58/CE, os quais contêm um conjunto de salvaguardas de proteção desses mesmos direitos fundamentais.

Tendo a Diretiva sido considerada inválida, afastaram-se consequentemente as derrogações nela previstas do artigo 5.º (confidencialidade das comunicações), do artigo 6.º (dados de tráfego), do artigo 9.º (dados de localização) da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas.

De igual modo, ficou sem efeito a alteração introduzida pelo artigo 11.º da Diretiva 2006/24/CE ao artigo 15.º da Diretiva 2002/58/CE, a qual excluía a aplicabilidade do n.º 1 do artigo 15.º aos dados conservados ao abrigo da Diretiva 2006/24/CE, esvaziando em grande parte a possibilidade aí admitida de os Estados membros adotarem medidas legislativas de restrição de direitos.

Com efeito, nos termos do n.º 1 do artigo 15.º da Diretiva 2002/58/CE, os Estados membros podem adotar medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nos artigos 5.º e 6.º, nos n.ºs 1 a 4 do artigo 8.º, e no artigo 9.º, incluindo a possibilidade de os dados serem conservados durante um período limitado, para fins designadamente de prevenção, deteção, investigação e repressão de infrações penais, sempre que essas restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática.

Por conseguinte, mesmo admitindo que, em execução do acórdão, a Lei n.º 32/2008, de 18 de julho, pudesse corresponder às medidas legislativas previstas no n.º 1 do artigo 15.º da Diretiva 2002/58/CE, na disponibilidade dos Estados membros, a lei nacional teria sempre de observar os princípios e acatar os limites impostos às restrições de direitos pelo artigo 15.º da Diretiva 2002/58/CE, interpretados à luz do seu Considerando 11.

Aí se desenvolve que as medidas a tomar pelos Estados membros devem estar em conformidade com a Convenção Europeia dos Direitos do Homem (CEDH), segundo a interpretação da mesma na jurisprudência do Tribunal Europeu dos Direitos do Homem. *Essas medidas devem ser adequadas, rigorosamente proporcionais ao objetivo a alcançar e necessárias numa sociedade democrática e devem estar sujeitas, além disso, a salvaguardas adequadas, em conformidade com a CEDH.*

Também o Considerando 2 da Diretiva 2002/58/CE oferece enquadramento geral para o tratamento de dados pessoais, reforçando que *esta diretiva visa assegurar o respeito dos direitos fundamentais e a observância dos princípios reconhecidos pela Carta dos Direitos Fundamentais da UE, em especial os direitos consignados nos artigos 7.º e 8.º da Carta.*

Sendo certo que a Carta vincula os Estados membros, por força do Tratado sobre a União Europeia, tendo por isso aqueles de respeitar os direitos e observar os princípios nela consagrados (cf. n.º 1 do artigo 51.º), a Lei n.º 32/2008, de 17 de julho, que transpôs a Diretiva 2006/24/CE para a ordem jurídica portuguesa, tem de ser avaliada na perspetiva da sua congruência com a Carta dos Direitos Fundamentais da UE.

O exercício que nos propomos aqui fazer consiste numa apreciação, ainda que sumária, da conformidade da Lei n.º 32/2008 com o Direito da UE, seguindo, especificamente, os fundamentos expostos no acórdão em relação às várias disposições da Diretiva e verificando se todos ou alguns deles se justificam quanto às normas da Lei portuguesa.

Começa-se por notar que a Lei n.º 32/2008, ao contrário da Diretiva, especifica os crimes cuja prevenção, deteção e repressão justifica a imposição deste tratamento de dados pessoais (cf. alínea g) do n.º 1 do artigo 2.º), e sujeita ainda a controlo judicial prévio o acesso aos dados pelas autoridades competentes (cf. alínea a) do n.º1 do artigo 7.º). Todavia, outros aspetos de regime sobre os quais incide o juízo de invalidade do Tribunal encontram-se previstos também na Lei nacional. Vejamos.

O TJUE reconhece que as medidas previstas na Diretiva, e que grosso modo correspondem à imposição do dever de conservação de dados de tráfego e de localização gerados no contexto de comunicações eletrónicas e do dever da sua transmissão a autoridades competentes para a finalidade de investigação, deteção e repressão de crimes graves, são legítimas e adequadas ao fim visado. Mas, quanto à necessidade de tais medidas, conclui pela violação do princípio da proporcionalidade nessa vertente.

O principal argumento em que assenta tal juízo prende-se com o facto de a conservação dos dados constituir uma restrição aos direitos fundamentais à vida privada e à proteção de dados pessoais (cf. §§26-27, 31, 33-34 do acórdão), não se excluindo a sua incidência no exercício da liberdade de expressão (cf. §28 do acórdão), e de afetar a totalidade da população. Ou seja, o tratamento de dados pessoais e consequente restrição daqueles direitos fundamentais abrange de maneira geral todas as pessoas, todos os meios de comunicação eletrónica e todos os dados relativos ao tráfego […] (§57 do acórdão), aplicando-se mesmo a pessoas em relação às quais não haja indícios que levem a acreditar que o seu comportamento possa ter um nexo, ainda que indireto ou longínquo, com infrações graves (§58 do acórdão), traduzindo-se tal conservação num tratamento automático de dados pessoais com risco significativo de acesso ilícito aos mesmos.

Sucede que a Lei n.º 32/2008 padece do mesmo vício.

O dever de conservação dos dados imposto às operadoras dos serviços de comunicação eletrónica respeita a todos os dados de tráfego e de localização de todos os clientes ou utilizadores das comunicações eletrónicas no território nacional. Sem que se atenda a um específico indício que permita associar uma pessoa a um concreto crime, mesmo que apenas como suspeito. E sem que se excecione deste dever de conservação os dados de tráfego e de localização daqueles que, nos termos de outros diplomas legais, estão vinculados e protegidos pelo segredo profissional (cf. §58 do acórdão).

Prevendo este diploma legal um tratamento de dados pessoais automático, relativo aos dados de todos os clientes ou utilizadores de comunicações eletrónicas, que não permite uma seleção dos dados sujeitos a conservação em função da ligação do seu titular, ainda que indireta, a crimes graves, nem permite excluir dessa conservação dados das pessoas que, legalmente, não podem ser objeto de controlo por estarem abrangidos pelo sigilo profissional, só pode concluir-se pela invalidade do mesmo por violação do princípio da proporcionalidade na restrição dos direitos ao respeito pela vida privada e à proteção dos dados pessoais (artigos 7.º e 8.º da Carta dos Direitos Fundamentais da UE).

Para além deste juízo geral de desnecessidade do tratamento de dados por ela previsto e imposto, a Lei n.º 32/2008 está também quanto a outros aspetos específicos em contradição com o Direito da União Europeia.

Desde logo, a Lei omite também, tal como a Diretiva, critérios objetivos que permitam definir o perfil e limitar o número das pessoas com autorização de acesso e de utilização posterior dos dados conservados ao estritamente necessário (cf. §62 do acórdão). Na verdade, a alínea d) do n.º 1 do artigo 7.º da Lei n.º 32/2008 não apresenta critérios que densifiquem o conceito de «pessoas especialmente autorizadas», limitando-se a repetir a fórmula consagrada na Diretiva e que foi objeto de censura pelo TJUE.

No que às medidas de segurança diz respeito, o mesmo artigo 7.º limita-se também a repetir, com algumas adaptações, o disposto no artigo 7.º da Diretiva, sem especificar regras quanto às medidas de segurança, nem as adaptar à quantidade, sensibilidade e especial risco de acesso ilícito (cf. §66 do acórdão).

Em relação ao prazo de conservação dos dados pessoais, embora a Lei, no seu artigo 6.º, preveja um prazo mais curto do que o máximo admitido pela Diretiva, não se indica qualquer elemento que permita compreender a razão de ser do prazo de um ano legalmente fixado – não sendo a opção legislativa neste ponto livre, por também estar sujeita ao princípio da proporcionalidade, sobram dúvidas quanto à observância do mesmo.

Em todos estas normas denota-se a ausência de especificação legal dos termos e condições em que pode ser realizado o tratamento de dados imposto, de modo a restringi-lo ao estritamente necessário à prossecução da respetiva finalidade, em clara violação do princípio da proporcionalidade.

Além disso, incorrendo no mesmo vício que a Diretiva, a Lei não impõe que os dados sejam conservados dentro do território da União, não estando assim garantida a fiscalização por entidades independentes como determina o n.º 3 do artigo 8.º da Carta dos Direitos Fundamentais da UE (cf. §68 do acórdão).

Em conclusão, a Lei n.º 32/2008 contém normas que preveem a restrição ou ingerência nos direitos fundamentais ao respeito pela vida privada e à proteção dos dados pessoais (artigos 7.º e 8.º da Carta dos Direitos Fundamentais da UE) com grande amplitude e intensidade em clara violação do princípio da proporcionalidade.

A terminar, duas observações. A primeira para sublinhar que a presente análise se limita à avaliação da conformidade da Lei n.º 32/2008 com a Carta dos Direitos Fundamentais da UE; mas a idêntica conclusão se chega se o padrão de avaliação for a Constituição da República Portuguesa: com os mesmos fundamentos, verifica-se uma restrição desproporcionada dos direitos à reserva da intimidade da vida privada e à proteção de dados pessoais, em violação do disposto no n.º 2 do artigo 18.º da Constituição. Aliás, têm-se sucedido nos Estados membros as declarações de inconstitucionalidade ou de invalidade das leis nacionais de retenção de dados.

A segunda observação prende-se com o alcance do acórdão do TJUE, que não se restringe a este concreto domínio da retenção de dados pessoais. Na verdade, a jurisprudência nele vertida repercute-se ainda em vários instrumentos jurídicos europeus e nacionais, os quais, na ânsia de satisfazerem de modo eficaz outros interesses relevantes, padecem precisamente do mesmo vício de fundo: a violação grosseira do princípio da proporcionalidade. Não pode, por isso, deixar de se alertar para a necessidade de se ter presente tal jurisprudência na apreciação da validade de outras normas jurídicas vigentes ou em preparação.

Clara Guerra e Filipa Calvão


DO
CUMEN
TOS

PARECER 9/2014 DO GRUPO DO ARTIGO 29.º*

SOBRE A APLICAÇÃO DA DIRETIVA 2002/58/CE AO *DEVICE FINGERPRINTING***

*) Parecer do Grupo de Trabalho de Proteção de Dados do Artigo 29.º, estabelecido nos termos do artigo 29.º da Diretiva de Proteção de Dados 95/46/CE, adotado a 25 de novembro de 2014

**) NT: optou-se por não traduzir esta expressão terminológica para evitar interpretações equívocas, como aliás aconteceu com outros termos, que foram preservados em Inglês em prol de uma melhor comunicação. *Device fingerprinting* (Tirar as impressões digitais do equipamento), como se verá ao longo do texto, é a possibilidade tecnológica de identificar inequivocamente um equipamento, através de um conjunto de características que o tornam único como se de uma impressão digital se tratasse.

1. SUMÁRIO

O *device fingerprinting* coloca graves preocupações de proteção de dados para os indivíduos. Certos serviços em linha propuseram-se recorrer ao *device fingerprinting* como uma alternativa aos *cookies*[1] HTTP para efeitos de fornecimento de analítica (*analytics*) ou para fins de rastreamento sem necessidade de obter o consentimento previsto no artigo 5.º, n.º 3, da Diretiva 2002/58/CE[2]. Isto demonstra que os riscos colocados pelo *device fingerprinting* não são teóricos e a investigação tem mostrado que o *device fingerprinting* já está a ser explorado[3].

Neste parecer, o Grupo de Trabalho do Artigo 29.º (G29) debruça-se sobre a questão do *device fingerprinting* e a aplicabilidade do artigo 5.º, n.º 3, da Diretiva 2002/58/CE, alterada pela Diretiva 2009/136/CE (Diretiva *e-Privacy*), sem prejuízo das disposições da Diretiva de Proteção de Dados 95/46/CE. A mensagem chave deste parecer é que o artigo 5.º, n.º 3, da Diretiva *e-Privacy* é aplicável ao *device fingerprinting*.

Este parecer alarga o âmbito do anterior Parecer 4/2012, sobre a isenção de consentimento para a utilização de *cookies,* e deixa claro aos terceiros[4] que processam *device fingerprints* geradas através do acesso ou armazenamento de informação no equipamento terminal do utilizador que apenas o podem fazer com o consentimento válido do utilizador (exceto se for aplicável uma isenção).

1) NT: *Cookies* - testemunhos de conexão

2) Wall Street Journal, 2013, *Web Giants Threaten End to Cookie Tracking*

3) Nikiforakis, 2013. *Cookieless Monster: exploring the ecosystem of web-based Device Fingerprinting*

4) Terceiros, na aceção do Considerando 66 da Diretiva 2009/136/CE

2. INTRODUÇÃO

O artigo 5.º, n.º 3, da Diretiva *e-Privacy* dispõe que os Estados membros devem assegurar que «o armazenamento de informações ou a possibilidade de acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador só sejam permitidos se este tiver dado o seu consentimento prévio com base em informações claras e completas, nos termos da Directiva 95/46/CE, nomeadamente sobre os objectivos do processamento»[5].

No Parecer 4/2012, o G29 apreciou a aplicação do artigo 5.º, n.º 3, da Diretiva *e-Privacy* em relação ao armazenamento ou acesso a informação através da utilização de *cookies*. O parecer esclarecia que o artigo 5.º, n.º 3, não se aplica exclusivamente a *cookies* mas é também aplicável a "tecnologias semelhantes".

O atual parecer debruça-se sobre os relatos crescentes que indicam estar em os terceiros a explorar ativamente tecnologias alternativas aos *cookies* para várias finalidades, numa tentativa de evitar a exigência de consentimento do artigo 5.º, n.º 3.

É especificamente analisado o cruzamento de um conjunto de elementos informativos, com vista à identificação inequívoca de determinados equipamentos ou aplicações, no que é designado por *device fingerprinting*.

As *device fingerprints* podem também constituir dados pessoais. Este parecer não analisa as disposições necessárias da Diretiva de Proteção de Dados, mas refere-se a questões de proteção de dados que são especialmente relevantes no contexto do *device fingerprinting*.

Tomemos como exemplo a situação em que há combinação de diversos elementos informativos, em particular identificadores únicos como os endereços IP, e a finalidade do tratamento é identificar os utilizadores, ao longo do tempo, através de vários sítios da *Web*, tal como acontece com a publicidade comportamental. Nestes casos, o tratamento de dados deve cumprir, de igual modo, as normas previstas na Diretiva de Proteção de Dados.

A tecnologia de *device fingerprinting* não está limitada aos parâmetros de configuração de um tradicional navegador de Internet num computador *desktop*. O *device fingerprinting* também não se encontra ligado a um protocolo específico, mas pode ser usado para detetar e registar um leque alargado de equipamentos ligados à Internet, eletrónica de consumo e aplicações, incluindo aquelas que correm nos equipamentos móveis, televisões inteligentes, consolas de jogos, leitores de livros eletrónicos, rádio pela Internet, sistemas no interior de veículos automóveis ou contadores inteligentes[6].

5) Tal não impede o armazenamento técnico ou o acesso que tenha como única finalidade efetuar a transmissão de uma comunicação através de uma rede de comunicações eletrónicas, ou que seja estritamente necessário ao prestador para fornecer um serviço da sociedade da informação que tenha sido expressamente solicitado pelo assinante ou pelo utilizador.

6) Por vezes referida como a "Internet das Coisas".

3. DEFINIÇÃO

O documento RFC6973[7] define uma *fingerprint* como "um conjunto de elementos informativos que identifica um equipamento ou aplicação". Este parecer usa o termo em sentido lato, isto é, como um conjunto de informação que pode ser usada, ao longo do tempo, para individualizar[8], relacionar[9] ou inferir[10] um utilizador, um agente utilizador ou um equipamento. Isto inclui, mas não exclusivamente, dados que derivam de:

a) A configuração de um *user agent*/dispositivo ou

b) Dados expostos pela utilização de protocolos de comunicação de rede.

Há muitos tipos de dados que podem formar uma *fingerprint*, incluindo os seguintes exemplos:

a) Informação CSS;

b) Objetos *JavaScript* (documento, janela, écran, navegador, data, língua);

c) Informação do cabeçalho HTTP (número de *bits de informação* na Linha *User Agent*, cabeçalho HTTP de encomenda, cabeçalho HTTP de variação por tipo de pedido);

d) Informação do relógio;

e) Variação de carga TCP;

f) Fontes instaladas;

g) Informação de *Plug-in* instalada (configuração e informação sobre a versão);

h) A utilização interna de Interfaces de Programação de Aplicações (API)[11], exposta pelo agente utilizador/equipamento; ou

i) A utilização externa de API de serviços *Web*, com os quais o agente utilizador/equipamento está a comunicar.

7) Cooper, 2013. Privacy Considerations for Internet Protocols, http://tools.ietf.org/html/rfc6973

8) *Singling out:* a possibilidade de isolar alguns ou todos os registos que identificam um individuo num conjunto de dados, Parecer 5/2014 do G29 sobre Técnicas de Anonimização, pp.11-12.

9) *Linkability*: a capacidade de relacionar, pelo menos, dois registos relativos ao mesmo titular ou a um grupo de titulares dos dados (quer numa mesma base de dados ou em duas bases de dados diferentes). Parecer 5/2014 do G29 sobre Técnicas de Anonimização, pp.11-12.

10) Inferência: a possibilidade de deduzir com probabilidade significativa o valor de um atributo de entre os valores de um conjunto de atributos. Parecer 5/2014 do G29 sobre Técnicas de Anonimização, pp.11-12.

11) A API oferece um ambiente amigável ao utilizador para aceder a funções ou rotinas dentro de uma componente de *software*.

4. ENQUADRAMENTO TÉCNICO

A Internet e a *Web* têm sido desenvolvidas tendo em mente a necessidade de uma arquitetura de rede flexível e aberta[12]. Devido às opções de desenho para ir ao encontro dessas necessidades, os equipamentos transmitem elementos informativos. Alguns protocolos integram uma variedade de elementos informativos obrigatórios e opcionais. O protocolo HTTP/1.1[13] contém campos no cabeçalho que permitem ao servidor e ao cliente incluir informação adicional relativa ao hipertexto. Alguns deles foram intencionalmente feitos para o servidor reconhecer tipos de clientes. Por exemplo, o campo no cabeçalho "pedido de *User-Agent*" inclui a seguinte descrição: «*isto destina-se a fins estatísticos, à deteção de violações de protocolo e ao reconhecimento automático de* user agents, *de modo a ajustar as respostas para evitar limitações específicas de* user agent.»

As utilizações típicas da Linha *User Agent* incluem a otimização da apresentação do conteúdo para um determinado tipo de equipamento, a utilização desta informação para marcar conteúdo para utilizadores específicos ou para recolher informação sobre o equipamento por motivos analíticos ou de segurança.

5. RISCOS DE PROTEÇÃO DE DADOS

Devido ao facto de um cabeçalho HTTP não ter habitualmente um valor único, os utilizadores só raramente podem ser individualmente identificados[14] a partir apenas de um elemento informativo. Os tipos de meios suportados por um navegador são frequentemente os mesmos entre os utilizadores que usam a mesma versão de navegador. Assim, mesmo quando processados isoladamente, estes elementos informativos não representam de um modo geral um risco para a proteção de dados.

Contudo, alguns elementos informativos podem ser combinados, criando um conjunto que é, por si só, suficientemente único (especialmente se combinados com outros identificadores como os endereços de IP de origem) para funcionar como uma impressão digital única do equipamento ou aplicação.

Tal impressão digital (*fingerprint*) permite distinguir um equipamento de outro e pode ser usada como uma alternativa encoberta aos *cookies* para rastrear, ao longo do tempo, o comportamento na Internet[15] [16] [17]. Daqui resulta que um indivíduo pode ser associado, e portanto identificado ou tornado identificável, pela impressão digital desse equipamento.

Os riscos do *device fingerprinting* para a proteção de dados são acrescidos pelo facto

12) Kahn, 1972. *Communications Principles for Operating Systems. Internal BBN memorandum.*

13) Fielding, Reschke, 2014. *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content.*

14) Há situações em que apenas um elemento informativo contém informação que pode identificar o titular dos dados, tal como o *token* de acesso OAuth.

15) *Panopticlick, Electronic Frontier Foundation, 2010.*

16) Yen, 2000. *Host Fingerprinting and Tracking on the Web: Privacy and Security Implications.*

17) Eckersley, 2010. *A Primer on Information Theory and Privacy.*

de o conjunto único de elementos informativos não estar apenas disponível ao editor do sítio *Web* mas também a muitos outros terceiros. Isto contrasta com a política da "mesma origem" dos *cookies* HTTP e é agravada pela natureza técnica da Rede, onde muitos terceiros contribuem para o conteúdo de uma página *Web*.

É comum que uma simples página *Web* seja dinamicamente gerada em tempo real pedindo conteúdo a múltiplas fontes. Cada um destes recursos irá gerar por si só pedidos HTTP, descarregando imagens, *JavaScript* e ficheiros CSS. Muitas páginas *Web* também contêm *web-bugs* e *tracking scripts*. Podem ainda emitir pedidos HTTP que registam sempre que o utilizador percorre ou clica numa página, imagem ou anúncio. Assim, os terceiros têm frequentemente a oportunidade de recolher a informação necessária para tirar a impressão digital do equipamento do utilizador.

Os riscos de proteção de dados não estão limitados ao rastreamento por terceiros. A combinação de dados obtida através das API presentes no *software* dos equipamentos dos clientes também coloca riscos de *device fingerprinting*. *Software*, plataformas e API diferentes oferecem cada um acesso a diferentes elementos informativos armazenados no equipamento. O navegador de Internet *Javascript* API, por exemplo, pode fornecer informação relativa ao tamanho do écran, à profundidade da cor e às fontes do sistema disponíveis. Outras API podem solicitar acesso aos elementos informativos armazenados no *firmware* (i.e. tipo de CPU), no sistema operativo (qual o seu tipo de SO) ou no modelo da placa gráfica[18]. As chamadas API podem igualmente revelar a presença de *software* instalado (como *plug-ins* do navegador) e qual a sua versão numérica exata. O acesso a estes conjuntos de informação aumenta o número de *bits* de informação (entropia) e, consequentemente, aumenta o risco de as pessoas serem reconhecidas através dos seus dispositivos[19].

Ao contrário dos *cookies* HTTP, o *device fingerprinting* pode operar de modo encoberto[20]. Não existem meios simples para os utilizadores impedirem esta atividade e são limitadas as oportunidades disponíveis para repor ou modificar quaisquer elementos informativos que estejam a ser usados para gerar a impressão digital. Por conseguinte, as *device fingerprints* podem ser usadas por terceiros para secretamente identificar ou individualizar os utilizadores com potencial para lhes ser dirigido conteúdo exclusivo ou, em todo o caso, para serem tratados de maneira diferenciada.

Foi assinalado no Parecer 16/2011[21] que as empresas de publicidade têm alegado que o uso de códigos únicos ou outros valores não envolve o tratamento de dados pessoais. Tal está em contradição com o facto de a finalidade do tratamento ser o fornecimento de conteúdos e anúncios personalizados, ou seja, de comunicar diretamente com um indivíduo específico. O G29 tem defendido em muitas ocasiões que tais identificadores únicos se qualificam como dados pessoais[22].

18) Mowery, 2012. *Pixel Perfect: Fingerprinting Canvas in HTML5.*

19) Mozilla, 2014. https://wiki.mozilla.org/Fingerprinting

20) Apenas em casos específicos, o protocolo exige um sinal ao utilizador, como a especificação de geolocalização HTML5 API .

21) Grupo de Trabalho do Artigo 29.º, 2011. Parecer 16/2011 sobre EASA/IAB Recomendação de melhores práticas para a publicidade comportamental em linha.

22) Grupo de Trabalho do Artigo 29.º, 2014. Parecer 5/2014 sobre Técnicas de Anonimização, págs. 11-12.

6. ENQUADRAMENTO LEGAL

Quando uma impressão digital (*fingerprint)* é gerada através do armazenamento ou do acesso a informação armazenada no equipamento terminal do utilizador, a Diretiva *e-Privacy* é aplicável.

Tal como descrito no Parecer 4/2012, o artigo 5.º, n.º 3, permite que o tratamento seja isento da obtenção de consentimento se um dos critérios seguintes for satisfeito:

CRITÉRIO A: armazenamento técnico ou acesso «que tenha como única finalidade efetuar a transmissão de uma comunicação através de uma rede de comunicações eletrónicas».

CRITÉRIO B: armazenamento técnico ou acesso «estritamente necessário ao prestador para fornecer um serviço da sociedade da informação que tenha sido expressamente solicitado pelo assinante ou pelo utilizador».

Além disso, o operador do sítio *Web* tem de respeitar o sentido de qualquer outro sinal indicador da preferência do utilizador, como por exemplo, o cabeçalho "Do-Not-Track"[23].

Embora a aplicação da Diretiva de Proteção de Dados esteja fora do âmbito deste parecer, sempre que o *device fingerprinting* implicar o tratamento de dados pessoais é importante que este seja feito em conformidade com as disposições respetivas desta Diretiva.

O artigo 5.º, n.º 3, da Diretiva *e-Privacy* estabelece a obrigatoriedade de obter consentimento do utilizador por parte de qualquer terceiro que pretenda armazenar ou aceder a informação armazenada no equipamento terminal do utilizador, mesmo que essa informação não seja ainda considerada como dados pessoais. O G29 apreciou esta questão do consentimento em vários pareceres, tanto em termos gerais[24], como especificamente em relação à publicidade comportamental em linha[25]. O G29 abordou também a obrigação de consentimento no contexto do artigo 5.º, n.º 3, e dos *cookies*[26].

Vale a pena relembrar o Parecer 2/2013 sobre as aplicações nos dispositivos inteligentes[27], o qual salientava:

23) W3C, Tracking Preference Expression (DNT). O protocolo Do-Not-Track (Não Rastrear) tem o potencial, em certas circunstâncias, de se tornar num mecanismo de consentimento granular, nos termos do Recital 66 da Diretiva 2009/136/CE, que permite aos utilizadores expressarem o consentimento através das configurações do seu navegador, mas apenas se o consentimento cumprir os requisitos acima mencionados de um consentimento válido.

24) Grupo de Trabalho do Artigo 29.º, 2011. Parecer 5/2011 sobre a definição de consentimento.

25) Grupo de Trabalho do Artigo 29.º, 2010. Parecer 2/2010 sobre a publicidade comportamental em linha.

26) Grupo de Trabalho do Artigo 29.º, 2013. Documento de Trabalho 2/2013 com orientações sobre como obter consentimento para os cookies.

27) Grupo de Trabalho do Artigo 29.º, 2013. Parecer 2/2003 sobre aplicações em dispositivos inteligentes, p.14

«*(…)a distinção entre o consentimento exigido para colocar quaisquer informações no dispositivo e ler informações armazenadas no dispositivo, e o consentimento necessário para haver fundamento jurídico para o tratamento de diferentes tipos de dados pessoais. Embora ambos os requisitos de consentimento sejam simultaneamente aplicáveis, (…)* é possível aglutinar os dois tipos de consentimento na prática (…) desde que o utilizador seja inequivocamente informado do objeto do seu consentimento».

O Considerando 66 da Diretiva *e-Privacy* refere-se a «*intromissão indevida na esfera privada*» e o artigo 5.º debruça-se sobre o requisito da confidencialidade das comunicações. O artigo 5.º, n.º 3.º, pode ser encarado como estendendo a confidencialidade da informação ao que está armazenado ou é acedido no equipamento do utilizador. Portanto, qualquer operação efetuada por terceiro que influencie o comportamento desse equipamento ou que, por qualquer outro modo, leve o equipamento a armazenar ou a dar acesso ou a expor informação encontra-se no âmbito do artigo 5.º, n.º 3.

O uso das palavras "armazenado ou acedido" indica que o armazenamento e acesso não precisam de ocorrer na mesma comunicação e não implica que tal seja realizado pela mesma parte. A informação que é armazenada por uma parte (incluindo informação armazenada pelo utilizador ou pelo fabricante do equipamento), e mais tarde acedida por outra parte, está, por conseguinte, abrangida pelo artigo 5.º, n.º 3.

Tome-se o exemplo de uma aplicação para telemóvel que processa a lista de contactos do utilizador: os contactos são armazenados pelo próprio utilizador mas o acesso é realizado por um terceiro. Não é correto interpretar-se esta situação, no sentido de que ao terceiro não é exigido que obtenha consentimento para aceder a esta informação simplesmente porque não foi ele a armazená-la. O requisito do consentimento é igualmente aplicável quando é acedida uma informação apenas com permissão de leitura (i.e. pedido do MAC *address* de uma interface de rede através de uma API do sistema operativo).

Assim, é importante que um terceiro tenha presente que sempre que o *device fingerprinting* implicar o armazenamento ou o acesso a (um conjunto de) informação no equipamento do utilizador, é necessário obter o seu consentimento (a menos que se aplique uma derrogação válida). Esta exigência mantém-se mesmo quando alguns dos elementos informativos não exigem o armazenamento ou o acesso à informação.

7. CENÁRIOS DE UTILIZAÇÃO

7.1 ANALÍTICA DE ORIGEM DO SÍTIO WEB

Alguns serviços em linha propuseram o *device fingerprinting* como uma alternativa aos *cookies* HTTP para fins de analítica, sem necessidade de obter o consentimento previsto no artigo 5.º, n.º 3. No Parecer 4/2012, o G29 reconheceu a necessidade de haver uma terceira isenção à exigência do consentimento quando a finalidade for a analítica de origem (*first-party analytics):*

«(…) *sempre que se limitem estritamente a fins próprios de estatísticas agregadas e quando são utilizados por sítios Web que já fornecem informações claras sobre estes testemunhos, conformes com a sua política de proteção da vida privada, bem como garantias adequadas de proteção da privacidade. Tais garantias deveriam incluir mecanismos de fácil utilização para excluir qualquer recolha de dados e tornar os dados completamente anónimos, a fim de serem aplicáveis a outros dados identificáveis recolhidos, tais como os endereços IP*».

Todavia, o parecer também afirmava que atualmente não há isenção ao consentimento para os *cookies* que se destinam exclusivamente a fins estatísticos, agregados e anonimizados, na origem[28]. Nesse sentido, a analítica de origem do sítio *Web* através de *device fingerprinting* não está abrangida pela isenção definida nos CRITÉRIOS A ou B, sendo o consentimento do utilizador requerido.

7.2 RASTREAMENTO PARA A PUBLICIDADE COMPORTAMENTAL EM LINHA

Muitos sítios *Web* contêm *web-bugs*, *pixel tags* e código *Javascript* de terceiros para permitir publicitar serviços. Isto resulta em vários pedidos de elementos informativos ao equipamento do utilizador. Os pedidos são transmitidos aos terceiros que fornecem os serviços publicitários e permite-lhes gerar uma impressão digital do equipamento para seguir os utilizadores, ao longo do tempo, através de vários sítios *Web*, criando um perfil de interesses para realizar publicidade direcionada, mesmo quando o utilizador rejeita os *cookies*. Este tratamento pode ser tecnicamente efetuado de modo encoberto, sem o conhecimento do utilizador.

O Parecer 4/2012 realça que a publicidade de terceiros não está abrangida pela isenção definida nos CRITÉRIOS A ou B. Assim, o *device fingerprinting* para fins de publicidade dirigida exige o consentimento do utilizador.

7.3 FORNECIMENTO DE REDE

A gestão correta de uma rede requer a transferência de certos elementos informativos relativos a cada equipamento da rede. Por exemplo, um ponto de acesso WI-FI que gere a conexão entre os equipamentos sem fios e uma rede com fios irá tratar alguns elementos informativos únicos e não únicos, como o *MAC address*[29] e o canal, de modo a manter corretamente as ligações e a encaminhar corretamente os pacotes de dados.

28) Grupo de Trabalho do Artigo 29.º, 2012. Parecer 4/2012 sobre a Isenção de consentimento para a utilização de testemunhos de conexão (*cookies*), págs. 10-11.

29) O *MAC address* será provavelmente único entre os equipamentos da rede. O prefixo do *MAC address* refere-se também ao dispositivo (*chip*) do fabricante.

Quando o fornecimento de rede requer elementos informativos que armazenam ou acedem a informações no equipamento do utilizador, então cai no âmbito do artigo 5.º, n.º 3. Sempre que este tratamento é exigido para o normal funcionamento da rede, considera-se ficar abrangido pela isenção do CRITÉRIO A.

A utilização secundária de um elemento informativo ou *device fingerprinting* para fins de rastreamento de atividade já não é considerada como tendo como «única finalidade efetuar a transmissão de uma comunicação através de uma rede de comunicações eletrónicas» ou como sendo «estritamente necessário ao fornecedor para fornecer um serviço da sociedade da informação que tenha sido expressamente solicitado pelo assinante ou pelo utilizador». A propósito da apreciação no Parecer 4/2012 dos *cookies* polivalentes, o G29 sublinhou que «é muito pouco provável que o rastreamento se ajuste aos *CRITÉRIOS A ou B*», portanto se um terceiro pretender usar o *device fingerprinting* para múltiplas finalidades, apenas estará «isento da obrigação de consentimento se todas as finalidades diferentes *(…) estiverem individualmente isentas dessa obrigação*».

7.4 ACESSO E CONTROLO DO UTILIZADOR

Um serviço em linha pode pretender usar *device fingerprinting* para apoiar o acesso e controlo do utilizador (i.e. em combinação com o nome de utilizador e a palavra-passe). O *device fingerprinting* pode ser usado para assegurar que uma conta está ligada a um equipamento específico, pelo que este funciona como um segundo fator de autenticação.

Vejamos. Um serviço de subscrição de música apenas permite que o utilizador aceda ao serviço a partir de um número limitado de dispositivos específicos. Se um utilizador tiver usado anteriormente um equipamento, o operador do sítio *Web* pode optar por realizar menos verificações antes de dar acesso.

Se uma impressão digital do equipamento é constituída por elementos informativos que armazenam e ganham acesso a informação existente no equipamento do utilizador, então encontra-se abrangida pelo âmbito do artigo 5.º, n.º 3. No entanto, neste caso, os fins não seriam considerados como «*estritamente necessários*» para fornecer uma funcionalidade explicitamente solicitada pelo utilizador; logo, o consentimento válido do utilizador é exigível.

Os operadores dos sítios *Web* talvez precisem de ponderar um conjunto de controlos adequados e proporcionados ou qualquer outro método de autenticação (por exemplo, uma palavra-passe de utilização única, confirmação de um *email* secundário).

7.5 SEGURANÇA CENTRADA NO UTILIZADOR

No Parecer 4/2012, o G29 entendeu que os *cookies* «*instalados especificamente para reforçar a segurança do serviço expressamente solicitado pelo utilizador*» (por exemplo, para detetar tentativas sucessivas falhadas de autenticação) estariam isentos ao abrigo do CRITÉRIO B.

Esta isenção também se aplicaria ao *device fingerprinting*, mas, assim como com os *cookies*, «não se aplica à utilização de técnicas relacionadas com a segurança de sítios Web nem a serviços de terceiros que não tenham sido expressamente solicitados pelo utilizador».

Se os dados são recolhidos através de *device fingerprinting* com o objetivo de oferecer segurança centrada no utilizador, para que se qualifiquem para a isenção de consentimento não podem ser utilizados para qualquer finalidade secundária. Têm de ser adotadas as salvaguardas técnicas e organizacionais para impedir qualquer uso secundário dos dados de *fingerprinting*, tipicamente mantidos em registos (*logs)* de segurança dos servidores.

7.6 ADAPTAÇÃO DA INTERFACE DO UTILIZADOR AO EQUIPAMENTO

Aceder à informação do equipamento, como o tamanho do écran, pode ser útil para otimizar a apresentação do conteúdo[30]. Um sítio *Web* de um órgão de comunicação social, por exemplo, pode comutar para um modo gráfico inferior ou para uma paginação a uma coluna perante um dispositivo móvel. Em alternativa, um sítio *Web* ou terceiros disponibilizando conteúdos através desse sítio poderiam procurar saber no equipamento quais as suas capacidades técnicas, nomeadamente quais os formatos de vídeo suportados.

Quando um terceiro pede acesso a informação armazenada no equipamento do utilizador, com o único propósito de adaptar os conteúdos às características do dispositivo, então o CRITÉRIO B é aplicável. Isto significa que para uma personalização de curta duração da interface do utilizador o consentimento não é exigível.

Contudo, se esta informação for também usada para fins secundários, a isenção deixa de ser aplicável.

30) Note-se que há outros métodos menos intrusivos para a privacidade para atingir o mesmo objetivo, tal como a utilização da linha *user-agent*.

8. CONCLUSÃO

Este parecer aprecia a questão do *device fingerprinting* e da aplicabilidade do artigo 5.º,n.º 3, da Diretiva da *e-Privacy* 2002/58/CE, alterada pela Diretiva 2009/136/CE, sem prejuízo das disposições da Diretiva de Proteção de Dados 95/46/CE.

Este parecer alarga a análise feita no Parecer 4/2012 sobre a isenção do consentimento para a utilização de *cookies* e corrobora que, em determinadas circunstâncias, a tecnologia leva a que seja obtido acesso ou armazenada informação no equipamento terminal do utilizador. O artigo 5.º, n.º 3, da Diretiva *e-Privacy* é igualmente aplicável ao nível do *device fingerprinting*.

Assim, quem pretender tratar as impressões digitais dos dispositivos, que são geradas a partir do acesso ou armazenamento de informação no equipamento terminal do utilizador, tem de obter primeiro o consentimento válido do utilizador, a menos que se aplique uma isenção.

Tradução de Clara Guerra

FICHA TÉCNICA

Título
Forum de Proteção de Dados

Proprietário e Editor
Comissão Nacional de Protecção de Dados

Diretor
Filipa Calvão

Sede da redação
Rua de São Bento, 148, 3º 1200-821 Lisboa

Periodicidade
Semestral

Tiragem
500 exs

Design e produção gráfica
Estrelas de Papel Lda.
Lisboa

ISSN 2183-5977

Julho 2015

Impresso em papel reciclado Munken Lynkx 120grs.

Isento de registo na ERC ao abrigo da alínea b) do artigo 12.º do Decreto Regulamentar n.º 8/99, de 9 de junho, alterado por último pelo Decreto Regulamentar n.º 2/2009, de 27 de janeiro.

PRÉMIO ENSAIO

DA COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS

Candidaturas até

31OUT. 2015

Aberto a trabalhos académicos e outros de investigação sobre proteção de Dados Pessoais

ÁREAS DAS CIÊNCIAS SOCIAIS E DAS CIÊNCIAS E TECNOLOGIAS

Regulamento disponível em **www.cnpd.pt**

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS