
CYBERLAW
by CIJIC

CYBERLAW by CIJIC

EDIÇÃO N.º VI – SETEMBRO/OUTUBRO DE 2018

REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

EDITOR: NUNO TEIXEIRA CASTRO

SUPORTE EDITORIAL: EUGÉNIO ALVES DA SILVA

PRESIDENTE DO CIJIC: EDUARDO VERA-CRUZ PINTO

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

CYBERLAW by CIJIC

NOTAS DO EDITOR:

No prólogo de mais esta nova edição da revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa, antecipo-me a aduzir dois actos, em breve, solenes, que não deverão passar em claro nas agendas de cada um.

O primeiro desses actos terá lugar no próximo 17 de Outubro na Universidade de Aveiro. Trata-se da Sétima edição da Iniciativa Portuguesa do Fórum da Governação da Internet.

Um sublinhado desde logo para o local do evento. É importante que a academia se sinta interligada com Portugal, no seu todo. Sair de Lisboa, do conforto centralizador da capital, é um pequeno mas mui nobre sinal de que há muito e bom trabalho a ser desenvolvido diariamente na plenitude dos mais de 98 mil quilómetros quadrados que compõem o nosso pequeno país.

No que à edição deste ano do Fórum da Governação da Internet diz respeito, trata-se de um evento organizado pela FCT (Fundação para a Ciência e a Tecnologia I.P), em parceria com a ANACOM (Autoridade Nacional de Comunicações), APDSI (Associação para a Promoção e Desenvolvimento da Sociedade da Informação), API (Associação Portuguesa de Imprensa), Associação DNS.PT, Ciência Viva (Agência Nacional para a Cultura Científica e Tecnológica), CNCS (Centro Nacional de Cibersegurança), IAPMEI (Agência para a Competitividade e Inovação), ISOC-PT

(Capítulo Português da ISOC), Polo TICE.PT, Secretaria Geral da Presidência do Conselho de Ministros, e Sociedade Civil.

Serão objecto de discussão, temas como «Governação e políticas públicas da Internet nos contextos nacional e global»; «Inteligência Artificial e *Big data*»; «Segurança no Ciberespaço: O dilema entre a privacidade do indivíduo e a segurança do Estado»; «Governação, confiança, privacidade e desafios na era do IoT»; «*Fake news, fake views* -Sociedade da (Des)Informação».

As sessões e respectivos painéis apresentam temas e oradores de reconhecida qualidade, e, seguramente, será um 17 de Outubro de 2018 muito e bem preenchido em Aveiro[1].

O outro evento, como seria natural, até pelo investimento feito pelo país na realização deste por mais dez anos em Portugal, é a *Lisboa web summit* 2018.

O programa e agenda[2] da feira, que se realizará no Altice Arena entre 5 e 8 de Novembro, já foram dados a conhecer. O destaque recai na presença de oradores como o Secretário-Geral das Nações Unidas, Sr. António Guterres; o inventor do *www*, Sir Tim Berners-Lee; o CEO do eBay, Mr. Devin Wenig; a Comissária Europeia para a Concorrência, Mrs. Margrethe Vestager; entre outros.

Os temas são vastos. A agenda *idem*. Uma semana desta feira para explorar avidamente.

Em suma, sendo eventos contrastantes na apresentação, na forma e até na finalidade, seria pouco cordial não aproveitar a proximidade destes para esta nota de agenda.

Arrolado o introito, focando-nos apenas no essencial desta nova edição, seguramente que a entrada em vigor, em pleno, do RGPD - *REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE*; bem como da Lei Geral de Protecção de Dados (LGPD) no Brasil, aprovada no plenário do

1 Informações sobre o programa do evento podem ser consultadas em: https://www.governacaointernet.pt/pdf/forum_programa_2018.pdf.
O evento é de entrada livre mas requer uma inscrição prévia. Mais informações em: https://www.governacaointernet.pt/2018.html
2 Mais informações em: https://websummit.com/schedule

Senado Federal pelo PLC 53/2018, a 10 de Julho; impuseram que o tema da protecção de dados pessoais fizesse, novamente, parte do cardápio da revista.

No plano nacional, a Proposta de Lei 120/XIII, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, continua em suave desenvolvimento[3], mais de dois anos após a publicação do Regulamento europeu, o RGPD.

Não obstante, procurando contrariar o *adagio* da Proposta de Lei 120/XIII, procuramos coligir doutrina e opinião que demonstrem um pouco do *vivace* de pessoas e organizações na adaptação às novas realidades supranacionais. Neste sentido, encontraremos *ways not to read* o RGPD; as principais dificuldades e dúvidas partilhadas por organizações e por pessoas singulares na adaptação à nova realidade jurídica europeia. *Curiosamente*, do outro lado do Atlântico, trazemos, ainda, o impacto da LGPD brasileira nos negócios e nas pessoas, neste novel quadro normativo de agregação temática. É, pela actualidade do tema, tempo, ainda, de reintegrar o conceito de desindexação, *in casu*, da desindexação de conteúdos ofensivos na net, recuperando críticas jurídicas ao relevante caso *Google Spain*.

Saltando da circunspecção dos dados pessoais e da privacidade para outro tema, serão apresentadas reflexões quanto à apreensão de correio eletrónico e registos de comunicação de natureza semelhante. O tema é fervilhante. Na actualidade, a vivência em sociedade cresce *digitalodependente*, convocando discussões doutrinárias profundas. Ainda não será desta que se pacificará, entre os intérpretes e aplicadores do direito, a distinção juridicamente relevante entre correio e correio eletrónico. Mas, as reflexões que aqui se publicam, valem a leitura e o crepitar de questões.

Colocada em perspectiva esta espécie de matrimónio, de conveniência, que o direito e a tecnologia assumiram, a problemática dos drones, inteligência artificial e robótica, também têm aqui palco no plano jurídico.

Direito e Tecnologia são meios essenciais ao desenvolvimento do homem, com implicações, dilacerantes, nas mais variadas formas em como revelamos o ser social que somos. A ética, juridicamente relevante, aliada à segurança - subjacente ao

3 Pode ser consultada a actividade relativa à Proposta de lei em: http://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=42368

conceito *Safe-by-design* (SbD) - estimulam dissecções imediatas desde o plano de concepção, no patamar R&D do desenvolvimento das mais diversas ferramentas, utensílios, *gadgets*, cada vez mais apetrechadas de inteligência artificial e robótica, que vão procurando satisfazer necessidades diversas do *mercado*, isto é, nossas.

Aproveitando a epígrafe, projecto uma questão, que gostava de ver discutida numa próxima edição da revista: será profícuo que ao invés da pirexia em torno da segurança - a qualquer custo - dos dispositivos, tentando antecipar toda a indeterminabilidade da vida humana – com todos os custos inerentes a esta tarefa de adivinhação – o foco poderia vir a incidir sobre a *responsabilidade pela segurança*? Assumindo-se a impossibilidade de segurança absoluta de toda e qualquer ferramenta, será que alvitraremos, no futuro, um modelo de responsabilidades partilhadas como solução?

A insolência típica das muitas questões não poderia terminar sem o regresso a uma ideia em processo de maturação: como conciliar diversas ordens, práticas e tradições jurídicas; actores, partes e contrapartes processuais; pessoas singulares, organizações e Estados, perante tal amálgama de situações quotidianas neste *pot-pourri* que a Internet é e do qual dependemos? Estaremos no vértice da necessidade de um Tribunal Internacional para a Internet? Mais umas penadas sobre a arquitetura de um desejável edifício de harmonização e resolução de pleitos jurídicos a nível mundial.

Resta-me, por fim, agradecer a todos pelo esforço e pelo trabalho, endereçando, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, um sentido reconhecimento a cada um dos autores: Muito Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

Boas leituras.

Lisboa, FDUL, 05 de Outubro de 2018

Nuno Teixeira Castro

CYBERLAW

by CIJIC

OPINIÃO

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS:

PRINCIPAIS DIFICULDADES E DÚVIDAS DAS ORGANIZAÇÕES E DOS TITULARES DE DADOS PESSOAIS NA ADAPTAÇÃO AO ATUAL REGIME

LURDES DIAS ALVES [1]

1Mestre em Direito (especialidade de Ciências Jurídicas). Doutoranda em Direito na Universidade Autónoma de Lisboa, onde investiga o tema: "*A proteção de dados pessoais e o sigilo bancário – A derrogação da privacidade*". Investigadora integrada no RATIO LEGIS - UAL. Cocoordenadora de Cursos de Formação e Pós-Graduações em Proteção de Dados Pessoais, Privacidade e Cibersegurança na UE, na Autónoma. Contacto: lurdes.dias.alves@gmail.com

Com a publicação em 4 de maio de 2016, e entrada em vigor em 25 de maio de 2016, o Regulamento Geral de Proteção de Dados (RGPD) contemplou, desde logo, um período transitório de dois anos para a sua aplicação plena, no regulamento, são consagradas no quadro europeu profundas alterações ao regime jurídico da defesa da privacidade das pessoas singulares.

Os Estados, as pessoas coletivas públicas e privadas, as organizações e os agentes económicos tiveram até 25 de maio de 2018 para preparar a adaptação às novas regras de proteção de dados. Contudo, raramente, diremos, a adaptação a um novo regime decorre sem dificuldades e dúvidas.

Passados quase cinco meses de plena aplicabilidade do RGPD, considera-se pertinente efetuar uma breve reflexão sobre as principais dificuldades e dúvidas das organizações e dos titulares dos dados pessoais na adaptação ao atual regime, destacamos como principais preocupações: *COMPLIANCE* – Como aferir e provar o cumprimento do RGPD; a questão do regime de reporte e divulgação em caso de *data breach*; o estatuto e perfil do *Data Protection Officer*; a diversidade e multiplicidade dos pedidos de consentimento; o excesso de direito de acesso por parte do Estado dos dados pessoais dos cidadãos; e, mas não menos importante, a falta de literacia em matéria de proteção de dados pessoais.

Para uma maior clarificação destas dificuldades e dúvidas, efetuaremos uma reflexão de forma sucinta quanto às dificuldades das organizações, por um lado, e as principais dúvidas dos titulares dos dados pessoais, por outro.

I. AS PRINCIPAIS DIFICULDADES DAS ORGANIZAÇÕES NA ADAPTAÇÃO AO ATUAL REGIME DE PROTEÇÃO DE DADOS PESSOAIS

O RGPD alterou por completo o paradigma da regulação em matéria de proteção de dados pessoais, passando de hetero-regulação para autorregulação. Uma dessas alterações introduzidas é o fim do controlo prévio exercido pela Autoridade Nacional (no caso português, a Comissão Nacional de Proteção de Dados – CNPD). Assim, o tratamento de dados pessoais deixa de ter a obrigatoriedade de comunicação e/ou autorização prévia.

É sobre o responsável pelo tratamento dos dados pessoais de cada organização que impende a obrigatoriedade do cumprimento do regulamento, e mais ainda, o responsável pelo tratamento tem de provar o cumprimento.

A - *COMPLIANCE* – Como aferir e provar o cumprimento do RGPD

Na verdade, uma das principais dificuldades que as organizações enfrentam é como aferir e provar que cumprem o regulamento. Uma das novidades introduzida pelo RGPD é o conceito de Avaliação de Impacto sobre a Proteção de Dados – AIPD ou PIA – *Privacy Impact Assessment* (conforme texto original do regulamento).

Mas o que é uma AIPD? Trata-se de um processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir e prevenir os riscos para os direitos e liberdades dos titulares dos dados pessoas decorrentes do tratamento, avaliando-os e determinando as medidas necessárias para fazer face aos riscos. As AIPD constituem importantes instrumentos em matéria de responsabilização, ao auxiliarem os responsáveis pelo tratamento não apenas a cumprir os requisitos do RGPD, mas também a demonstrar que foram tomadas medidas adequadas para assegurar a conformidade com o regulamento (*i.e.* uma AIPD é um processo que visa aferir e provar a conformidade do tratamento de dados).

Porém, não é obrigatório realizar uma AIPD para todas as operações de tratamento. Só existe essa obrigação quando o tratamento for «*suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares*». Para aferir quais são as operações de tratamento «*suscetíveis de implicar um elevado risco*», devem ser considerados nove critérios: 1. Avaliação ou classificação, incluindo definição de perfis e previsão, em especial de «*aspetos*

relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados»; 2. Decisões automatizadas que produzam efeitos jurídicos ou afetem significativamente de modo similar: tratamento destinado à tomada de decisões sobre os titulares dos dados e que produza «*efeitos jurídicos relativamente à pessoa singular*» ou que «*a afetem significativamente de forma similar*»; 3. Controlo sistemático: tratamento utilizado para observar, monitorizar ou controlar os titulares dos dados, incluindo dados recolhidos através de redes, ou um «*controlo sistemático de zonas acessíveis ao público*»; 4. Dados sensíveis ou dados de natureza altamente pessoal: inclui categorias especiais de dados pessoais (definido nos art.ºs 9.º e 10.º do RGPD); 5. Dados tratados em grande escala: (*v.g.* a) o número de titulares de dados envolvidos, quer através de um número específico quer através de uma percentagem da população pertinente; b) o volume de dados e/ou a diversidade de dados diferentes a tratar; c) a duração da atividade de tratamento de dados ou a sua pertinência; d) a dimensão geográfica da atividade de tratamento.) 6. Estabelecer correspondências ou combinar conjuntos de dados: (*v.g.* dados de duas ou mais operações de tratamento, com diferentes finalidades e/ou efetuadas por diferentes responsáveis pelo tratamento de dados de tal forma que excedam as expectativas razoáveis do titular dos dados aquando do consentimento); 7. Dados relativos a titulares de dados vulneráveis: o tratamento deste tipo de dados constitui um critério devido ao acentuado desequilíbrio de poder entre os titulares dos dados e o responsável pelo tratamento dos dados, significando isto que os indivíduos podem não ser capazes de consentir, ou opor-se, facilmente ao tratamento dos seus dados ou de exercer os seus direitos (*v.g.* dados de crianças; dados dos trabalhadores no contexto laboral; pessoas com doenças mentais; requerentes de asilo; idosos; doentes, etc.); 8. Utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais (*v.g.* a utilização da impressão digital e do reconhecimento facial para melhorar o controlo do acesso físico, etc.), aliás, o RGPD alerta que a utilização de uma nova tecnologia pode implicar a obrigatoriedade de realização de uma AIPD; 9. Quando o próprio tratamento impede os titulares dos dados de exercer um direito ou de utilizar um serviço ou um contrato (*v.g.* numa operação de tratamento destinada a autorizar, alterar ou recusar o acesso dos titulares dos dados a um serviço ou que estes celebrem um contrato.

Impõe-se que seja desmistificada a obrigatoriedade sistemática de uma AIPD, desde logo porque os responsáveis pelo tratamento de dados devem encarar a realização de uma AIPD como uma avaliação útil e positiva que ajusta o tratamento de dados efetuado com a

conformidade jurídica, ao invés de a encararem como um custo adicional e uma tarefa desnecessária.

B - A questão do regime de reporte e divulgação em caso de *data breach*

Uma outra questão, não menos relevante, que tem gerado grande preocupação e dificuldade, é a que concerne a melhor interpretação do prazo máximo de 72 horas estabelecido para comunicação e reporte de falhas ou violação de dados (*data breach* no texto original do regulamento). Note-se que é consensual considerar a falta de reporte e comunicação de falhas ou violação de dados uma das questões passíveis de levar à aplicação das sanções elevadas, as quais podem facilmente ascender a 20 milhões de euros.

O problema reside essencialmente na interpretação de «quando é que um responsável pelo tratamento tem conhecimento de *data breach*, qual o momento que se deve ter em conta para a notificação?». Deverá considerar-se que um responsável pelo tratamento tem «conhecimento» quando tem um grau razoável de certeza de que ocorreu um incidente de segurança que afetou dados pessoais. Porque o RGPD exige que o responsável pelo tratamento aplique todas as medidas técnicas de proteção e de organização para apurar imediatamente a ocorrência de uma violação e para informar rapidamente a autoridade de controlo e os titulares dos dados. Deverá ainda comprovar que a notificação foi enviada sem demora injustificada e importa ter em conta, em especial, a natureza e a gravidade da violação e as respetivas consequências e efeitos adversos para o titular dos dados.

Em caso de *data breach* o responsável pelo tratamento fica obrigado a assegurar que terá, sempre, «conhecimento» de eventuais violações em tempo útil, para que possa tomar medidas adequadas. O que não se mostra de difícil apuramento e muito menos impossível, até porque as circunstâncias de uma violação irão ditar as condições exatas em que se pode considerar que um responsável pelo tratamento tem «conhecimento» dessa violação. Casos há em que é relativamente evidente desde o início se tal ocorreu. Todavia, a maior preocupação não deve ser centrada na prova de momento do «conhecimento» da violação de dados, mas sim na ação imediata para investigar o incidente, o que originou a falha ou violação, a fim de determinar se os dados pessoais foram de facto violados e tomar medidas de reparação e notificação.

C - O estatuto e perfil do *Data Protection Officer*

Outro conceito introduzido é a figura do Encarregado de Proteção de Dados – EPD (ou *Data Protection Officer* como é definido no texto original do regulamento). Esta nova figura tem criado sérias dúvidas nas organizações quanto à obrigatoriedade da sua designação; se um único grupo organizacional tem de nomear um único EPD ou um para cada organização; se tem de ser interno ou externo; em que local terá de estar domiciliado; quais os requisitos e qualidades profissionais; quais os recursos que o responsável pelo tratamento de dados deverá disponibilizar ao EPD; quais as salvaguardas ao dispor do EPD para desempenhar as suas funções com independência; qual a responsabilidade do EPD em caso de incumprimento dos requisitos impostos pelo RGPD; qual o papel do EPD numa AIPD – tudo isto entre outras dúvidas com que as organizações se têm deparado.

Desde logo, só é obrigatória a designação de um EPD, se: o tratamento for efetuado por autoridade ou organismo público (exceto os tribunais no exercício da sua função jurisdicional); as atividades principais do responsável pelo tratamento ou do subcontratante consistirem em operações de tratamento que exijam controlo regular e sistemático dos titulares dos dados em grande escala; e se as atividades principais do responsável pelo tratamento ou do subcontratante consistirem em operações de tratamento em grande escala de categorias especiais de dados ou de dados pessoais relacionados com condenações penais e infrações. Ainda assim, mesmo que não seja obrigatório designar um EPD, as organizações poderão considerar conveniente designar um EPD, a título voluntário.

Ressalva-se que um grupo empresarial ou organizacional pode designar um único EPD, desde que este esteja «*facilmente acessível a partir de cada estabelecimento*». O requisito essencial é exatamente a acessibilidade: o EPD tem de estar acessível e contactável em relação aos titulares dos dados, à autoridade de controlo e, naturalmente, à organização ou grupo organizacional.

O EPD pode ser um elemento do pessoal da entidade responsável pelo tratamento ou do subcontratante (EPD interno), ou exercer as suas funções com base num contrato de prestação de serviços (EPD externo). E, para que se assegure que o EPD esteja acessível, é aconselhável que esteja domiciliado na União Europeia.

Deve ser designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio das normas e práticas de proteção de dados, bem como na sua capacidade para desempenhar as respetivas funções. Salienta-se que deve ter

competências no domínio das normas e práticas de proteção de dados nacionais e europeias, incluindo um conhecimento profundo do RGPD, e conhecimentos das operações de tratamento efetuadas, das tecnologias da informação e da segurança dos dados e do setor empresarial e da organização; finalmente, é importante que tenha a capacidade para promover uma cultura de proteção de dados no seio da organização.

Para que o EPD desempenhe as suas funções com total independência é necessário que os responsáveis pelo tratamento ou subcontratantes não transmitam instruções relativas ao exercício das funções do EPD. Acresce que o responsável pelo tratamento não pode destituir nem penalizar o EPD pelo exercício das suas funções. Geralmente, os cargos suscetíveis de gerar conflitos com o EPD no seio da organização podem incluir não só os cargos de gestão superiores (*v.g*. diretor executivo, diretor de operações, diretor financeiro, diretor do departamento médico, diretor de marketing, diretor dos recursos humanos ou diretor informático).

Ao EPD devem ser facultados os recursos necessários ao desempenho das suas funções face à natureza das operações de tratamento e das atividades e dimensão da organização (*i.e.*: apoio ativo às funções do EPD por parte dos quadros de gestão superiores; tempo suficiente para que os EPD desempenhem as suas tarefas; apoio adequado em termos de recursos financeiros, infraestruturas e pessoal adstrito à sua equipe de trabalho; deve ser comunicada oficialmente a nomeação do EPD a todo o pessoal; acesso a outros serviços no seio da organização, para que o EPD possa receber apoio, contributos ou informações essenciais por parte destes outros serviços; tem igual relevância a garantia de formação contínua).

Atente-se que o EPD não é pessoalmente responsável pelo incumprimento dos requisitos de proteção de dados: compete ao responsável pelo tratamento ou ao subcontratante assegurar e poder comprovar que o tratamento respeita o Regulamento aplicável. Porém, relativamente à avaliação de impacto sobre a proteção de dados, o responsável pelo tratamento ou o subcontratante deve solicitar o parecer do EPD, sempre que seja questionado se se deve ou não efetuar a AIPD; qual a metodologia a seguir na realização da AIPD; se deve realizar a AIPD internamente ou externalizá-la; quais as salvaguardas (incluindo medidas técnicas e organizativas) a aplicar no sentido de atenuar os eventuais riscos para os direitos e interesses dos titulares de dados; se a avaliação de impacto sobre a proteção de dados foi ou não corretamente efetuada e se as suas conclusões (se o tratamento deve ou não ser realizado e quais as salvaguardas a aplicar) estão em conformidade com os requisitos de proteção de dados.

II. AS DÚVIDAS DOS TITULARES DE DADOS PESSOAIS

O RGPD, apesar de encerrar em si muitos princípios, regras gerais, direitos e obrigações que já constavam da Diretiva 95/46/CE, veio introduzir importantes alterações: entre outras, e talvez a mais notória em termos jurídicos, temos o grau de intensificação do processo e requisitos aplicáveis à obtenção do consentimento do titular de dados pessoais nas mais diversas operações de tratamento de dados, fomentando a obrigatoriedade de demonstrar se o consentimento obtido pelo responsável pelo tratamento, e se respeita todos os novos requisitos – em caso negativo, será imprescindível obter novo consentimento do titular dos dados pessoais em conformidade com as disposições do RGPD, sob pena de o tratamento se tornar ilícito por falta de fundamento jurídico.

A - A diversidade e multiplicidade dos pedidos de consentimento

Um pedido de consentimento tem de ser apresentado ao titular dos dados pessoais de forma clara e concisa, utilizando uma linguagem de fácil compreensão, e de modo que o distinga claramente de outras informações, como os termos e condições do serviço. O pedido tem de especificar qual a utilização que será dada aos dados pessoais recolhidos e tem de incluir os contactos do responsável pelo tratamento de dados.

Atente-se, pois, que a legitimidade para o tratamento de dados pessoais advém da licitude na obtenção do consentimento do titular dos dados, e este consentimento somente é lícito - logo válido - se corresponder a uma *manifestação de vontade*, *livre*, específica, *informada* e *explícita*, pela qual o titular dos dados aceita o tratamento *mediante declaração* ou *ato positivo inequívoco*.

Conforme estabelece o n.º 1 do art.º 6.º do RGPD quanto aos requisitos conducentes à verificação da licitude para o tratamento de dados pessoais, o tratamento é lícito se o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas. E se o tratamento for necessário para: **(i)** a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; **(ii)** o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; **(iii)** a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; **(iv)** o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; **(v)** efeito dos interesses legítimos

prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

Para que se considere que o consentimento é informado, o responsável pelo tratamento tem de demonstrar que o titular dos dados recebeu, pelo menos, as seguintes informações sobre o tratamento: **a)** a identidade do responsável pelo tratamento dos dados; **b)** os fins para os quais os dados irão ser tratados; **c)** o tipo de dados que serão tratados; **d)** a possibilidade de retirar o consentimento dado (v.g., enviando uma mensagem de correio eletrónico para retirar o consentimento); **e)** se aplicável, o facto de os dados irem ser utilizados para decisões exclusivamente automatizadas, incluindo a definição de perfis; **f)** informações destinadas a apurar se o consentimento está relacionado com uma transferência internacional dos dados, os possíveis riscos de transferências de dados para fora da UE se tais países não estiverem sujeitos a uma decisão de adequação da Comissão e não existirem garantias adequadas.

Os titulares dos dados pessoais têm, de facto, sido confrontados com inúmeros, diremos demasiados, pedidos de consentimento, muitos dos quais desnecessários e que refletem as dificuldades e dúvidas por parte dos responsáveis pelo tratamento; a este propósito, diga-se que, se o consentimento dado por uma pessoa antes do RGPD ser aplicável estiver em conformidade com as condições e os requisitos do regulamento, não é necessário ser solicitado de novo o consentimento. Só é necessário um novo consentimento se a organização obteve o consentimento dos seus clientes há alguns anos utilizando um sistema de opções pré-validadas *online*. Este modelo de obtenção de consentimento deixou de ser válido em 25 de maio de 2018 - logo, o responsável pelo tratamento terá de obter um novo consentimento, caso pretenda continuar a efetuar o tratamento dos dados.

B - O excesso de direito de acesso por parte do Estado dos dados pessoais dos cidadãos

Se por um lado aplaudimos o cruzamento de informação na administração pública com vista à celeridade processual, por outro lado, este cruzamento de informação não mais é que uma transmissão de dados de uma organização para outra, sendo que o consentimento dado pelo titular dos dados tinha uma finalidade diversa daquela que se verifica após a transmissão de dados.

Na maioria das vezes estão em causa dados pessoais sensíveis (*v.g.* dados de saúde, dados genéticos, dados familiares, dados de crédito e solvabilidade, entre outros não menos importantes) que requerem uma proteção jurídica acrescida pela natureza dos direitos fundamentais em causa.

A maior dúvida neste âmbito reside primordialmente na ausência (por completo ou parcial) do nível de acesso, por parte dos funcionários da administração pública, a dados referentes à reserva da intimidade da vida privada e familiar.

C - A falta de literacia em matéria de proteção de dados pessoais

É indubitável que vivemos numa sociedade assente na tecnologia – e, por exemplo, basta pensar nas câmaras de videovigilância em grande parte do espaço público e privado; no modo como as instituições de crédito e sociedades financeiras sabem onde e como gastamos o nosso dinheiro (mais ainda, sabem como o ganhamos); como as grandes superfícies sabem os produtos que consumimos, quais os nossos gostos e tendências, ao ponto de poderem definir um perfil pessoal dos nossos hábitos e rotinas; os «*radares*» e a «*via verde*», que sabem por onde nos deslocamos e para onde viajamos; máquinas de «*raio X*» nos aeroportos, que visualizam os nossos pertences (e até o nosso corpo); a utilização de «*cookies*», que permite determinar a nossa utilização e navegação na internet (a tão usualmente designada pegada digital) - estas, entre muitas outras situações, mostram a variedade de casos em que, voluntária ou involuntariamente, a nossa privacidade fica mitigada ou até mesmo comprometida.

Nos últimos anos tem-se assistido a um crescimento exponencial do volume de dados gerados por sistemas de informação, ligados em rede e que geram dados, de tráfego e de conteúdo, interligados e a uma velocidade não antes imaginável. Com efeito, o elevado número de recolha, tratamento e troca de dados pessoais que atualmente ocorre, advém da maior disponibilização de informações privadas, cedidas, voluntária ou involuntariamente, pelas próprias pessoas (pelos próprios titulares dos dados pessoais), nomeadamente nas redes sociais.

Atualmente, em todo o mundo, sobretudo nos países desenvolvidos, os cidadãos não só são perseguidos continuamente no dia-a-dia, como consentem, de livre vontade, na divulgação dos seus próprios dados, satisfazendo o «*voyeurismo*» da sociedade contemporânea. Não restem dúvidas: nas últimas décadas assistimos a uma revolução digital que tornou a sociedade numa sociedade de informação, mas também de exposição.

A tutela da vida privada exige, hoje, mais transparência e controlo no concernente ao tratamento de dados por empresas e autoridades públicas. Ainda assim, teremos de levar em linha de conta os comportamentos das pessoas, que paradoxalmente estão menos cientes do seu direito à privacidade, permitindo a divulgação, e divulgando ela mesmo, informações pessoais, sem consciência das reais implicações dos seus atos, em redes totalmente abertas, nas quais não há controlo nem fiscalização.

Consideramos que, é imprescindível sensibilizar os indivíduos para a autoproteção da privacidade; os utilizadores das novas tecnologias devem estar cientes dos perigos que estas comportam e, nomeadamente, devem ter consciência de que a divulgação de informações em redes abertas escapa ao seu controlo. Os seus dados, uma vez disponibilizados, estão para sempre disponíveis. Por isso mesmo, a privacidade, uma vez perdida, está perdida para sempre. Por isso, as novas tecnologias de informação impõem que o direito à privacidade seja repensado e reconfigurado como um direito ao anonimato.

De facto, nesta sociedade cada vez mais aberta, e adepta da era digital, onde se expõe com toda a abertura a vida privada, e até a vida familiar, deixou de fazer sentido a privacidade, tal como a conhecemos. Na verdade, assistimos a mudanças de mentalidade e de comportamento social em que o valor da proteção da privacidade deixou de ser um «*bem supremo*», deixando até desvanecer a noção e o valor de que a privacidade é um direito inerentemente humano e um pré-requisito para a manutenção da condição humana com dignidade e respeito. Cumpre, pois, refletir sobre a dimensão, jurídica, ética e social, desta realidade.