O NOVO REGULAMENTO DE PROTEÇÃO DE DADOS – AS PRINCIPAIS ALTERAÇÕES[1]

JORGE BARROS MENDES[2]
Docente na Escola Superior de Tecnologia e Gestão do IPLeiria
Investigador no CIEJE-IPLeiria. Advogado

EXCERTOS

"A evolução tecnológica, com sistemas de informação cada vez mais eficientes, levou a que os nossos dados pessoais proliferassem na rede e nas organizações, sem que a maior parte das vezes o seu titular disso tenha noção"

"Sucede que a elaboração e publicação do Regulamento Geral de Proteção de Dados foi um processo moroso e complicado. Verdadeiramente foram necessários quatro anos para que existisse consenso e o GDPR fosse publicado"

"O GDPR aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a ele destinados"

"Sempre que os dados pessoais forem suscetíveis de ser legitimamente comunicados a outro destinatário, o titular dos dados deverá ser informado aquando da primeira comunicação dos dados pessoais a esse destinatário"

"A figura do encarregado de proteção de dados, comumente designado de DPO, está consagrada no artigo 37º do GDPR"

"Os poderes de investigação em matéria de acesso às instalações deverão ser exercidos em conformidade com os requisitos específicos do direito processual do Estado-membro"

Introdução

O Regulamento Geral sobre a Proteção de Dados foi publicado no jornal oficial da União Europeia no dia 4 de maio de 2016. Este diploma legal revogará a legislação atualmente em vigor sobre a proteção de dados pessoais, publicada em 1995, e todas as suas regras terão de estar implementadas pelas empresas até ao dia 28 de maio de 2018. O objetivo do regulamento é o de proteger a privacidade dos cidadãos e garantir a livre circulação de dados pessoais dentro da União Europeia.

Em paralelo com a aplicação de novos direitos para os cidadãos, o novo regulamento liberta as empresas dos pedidos de autorizações de tratamento de dados junto da Comissão Nacional de Proteção de Dados (CNPD), mas define novos requisitos no processamento da informação, uma vez que terão de ser mantidos registos sobre tratamentos de dados que são efetuados. Terão de ser revistas as políticas de privacidade e estas passarão a ser numa linguagem clara e percetível. O regulamento cria a figura do encarregado da proteção de dados (*data protection officer*) que será o agente de ligação com a CNPD, nomeadamente quando existam quebras de segurança.

1. Ponto prévio

A evolução tecnológica, com sistemas de informação cada vez mais eficientes, levou a que os nossos dados pessoais proliferassem na rede e nas organizações, sem que a maior parte das vezes o seu titular disso tenha noção.

Em 1980, o Conselho da Europa, através da Convenção 108[3], e a Organização para a Cooperação e Desenvolvimento Económico tentaram estabelecer as linhas orientadoras no âmbito da proteção de dados pessoais em termos internacionais. Veja-se que no preâmbulo de tal texto é afirmado perentoriamente que *"é desejável alargar a proteção dos direitos e das liberdades fundamentais de todas as pessoas, nomeadamente o direito ao respeito pela vida privada, tendo em consideração o fluxo crescente, através das fronteiras, de dados de carácter pessoal susceptíveis de tratamento automatizado"*.

Desde logo se estabelecia no artigo 4º que os países deveriam adotar no seu direito interno as medidas necessárias com vista à aplicação dos princípios básicos para a proteção de dados.

Nesta senda, em termos europeus, a Diretiva 95/46/CE, do Parlamento e do Conselho, de 24 de outubro, tentou criar uma harmonização da defesa dos direitos e das liberdades das pessoas singulares e assegurar a livre circulação de dados pessoais entre os Estados-membros. Aliás, no Considerando 11 e 12 da sobredita diretiva estabelecia o diploma que "*11) Considerando que os princípios da proteção dos direitos e liberdades das pessoas, nomeadamente do direito à vida privada, contidos na presente diretiva, precisam e ampliam os princípios contidos na Convenção do Conselho da Europa, de 28 de Janeiro de 1981, relativa à proteção das pessoas no que diz respeito ao tratamento automatizado de dados pessoais; 12) Considerando que os princípios da proteção devem aplicar-se a todo e qualquer tratamento de dados pessoais sempre que as atividades do responsável pelo tratamento sejam regidas pelo direito comunitário (…), pelo que aquilo que foi tentado pelo legislador europeu foi proceder a uma harmonização a nível europeu em sede de proteção de dados.*"

O Tribunal de Justiça da União Europeia[4], por diversas vezes, salientou que "*a Diretiva 95/46/CE visa tornar equivalente em todos os Estados-Membros o nível de proteção dos direitos, liberdades das pessoas no que diz respeito ao tratamento de dados pessoais, uma aproximação das legislações nacionais aplicáveis na matéria não deve fazer diminuir a proteção que asseguram, devendo, pelo contrário, ter por objetivo garantir um elevado nível de proteção na União e uma harmonização das referidas legislações nacionais não se limita a uma harmonização mínima, mas conduz a uma harmonização que é, em princípio completa*"[5].

A Carta dos Direitos Fundamentais da União Europeia[6], no seu artigo 8º, consagra expressamente que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhe digam respeito e que tais dados só podem ser objeto de tratamento leal para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento expressamente previsto na lei. Consagra ainda a faculdade de todas as pessoas poderem aceder aos dados que lhes digam respeito e que foram coligidos e ainda de retificação dos mesmos, ficando o incumprimento

de tais direitos sujeito à fiscalização por parte de uma entidade administrativa independente.

O Tratado sobre o Funcionamento da União Europeia, na versão do Tratado de Lisboa, estabeleceu no seu artigo 16º que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. Mais estabelece no seu n. 2: "*O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes*."

Ora, foi aqui aberto o caminho para que viesse a ser elaborado o Regulamento (EU) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril.

Sucede que a elaboração e publicação do Regulamento Geral de Proteção de Dados[7] foi um processo moroso e complicado. Verdadeiramente foram necessários quatro anos para que existisse consenso e o GDPR fosse publicado.

Tenha-se em atenção que todo o andamento de revisão das normas relativas aos dados pessoais teve início em maio de 2009, com a realização de uma conferência promovida pela Comissão Europeia dedicada à proteção de dados. O objetivo da comissão foi o de discutir a transferência de dados a nível internacional e a perigosidade deste fluxo, nomeadamente devido ao incremento da mobilidade e das telecomunicações.

Esta conferência levou a que em dezembro do mesmo ano o grupo de trabalho do artigo 29º[8] publicasse um relatório, "O Futuro da Privacidade", a pedido da Comissão Europeia – nesse relatório, o WP29 alertava para a necessidade de uma melhor aplicação dos princípios de proteção dos dados pessoais, nomeadamente atenta a modernização tecnológica que se vinha a sentir.

Um ano depois, em novembro de 2010, a Comissão Europeia estabeleceu a estratégia para a proteção dos dados pessoais nas áreas políticas, tendo como objetivo o de reduzir a burocracia para os

negócios e garantir a livre circulação de dados na União Europeia. Esta revisão de políticas destinou-se a ser utilizada pela comissão, tendo por base uma consulta pública com o escopo de se proceder à revisão da diretiva europeia de proteção de dados.

Sucede que em junho de 2011, sob a liderança do deputado alemão Axel Voss, do Comité das Liberdades Cívicas, da Justiça e dos Assuntos Internos[9], foi aprovada uma proposta intitulada de "Uma abordagem abrangente da proteção de dados pessoais na UE" como reação à comunicação da Comissão Europeia sobre o futuro da legislação europeia em matéria de proteção de dados. O tópico chave era a alteração da Diretiva de Proteção de Dados existente, ou seja, o texto de 1995.

No entanto, o grande mote para a reforma da proteção de dados pessoais viria a ser dado a 17 de novembro de 2011, na sessão de abertura da 35ª Conferência de Privacidade da Associação Alemã de Proteção de Dados e Segurança de Dados (GDD), em que Paul Nemitz, diretor para os Direitos Fundamentais e Cidadania da Comissão Europeia, anunciou que a Comissão Europeia planeava implementar um regulamento, diretamente aplicável a todos os Estados-membros da União Europeia, com o objetivo de harmonizar as leis de proteção de dados em toda a Europa.

E tal intenção da Comissão foi anunciada em 25 de janeiro de 2012. A Comissão propôs, então, a realização de uma reforma abrangente das normas de proteção de dados da União de 1995, com o objetivo de fortalecer os direitos de privacidade, sobretudo tendo em vista as questões informáticas e da internet, e impulsionar a economia digital da Europa, e isto porque o progresso tecnológico e a globalização alteraram profundamente a forma como nossos dados são recolhidos, acedidos e utilizados.

Ora, proceder à alteração da legislação existente e proceder à harmonização das normas em termos europeus foi um percurso difícil, especialmente pelo lobby e as pressões políticas exercidas junto da Comissão Europeia – veja-se, por exemplo, que a 21 de fevereiro de 2012 era noticiado pela Euractiv que os Estados Unidos da América estavam a ser muito ativos na tentativa de alterar o projeto de legislação apresentado. Pretendiam proteger o interesse das empresas dos EUA

que operam na União Europeia e, consequentemente, o texto proposto pela Comissão foi significativamente alterado antes mesmo de chegar ao Parlamento Europeu e ao Conselho para apreciação.

Em 2012, o WP29 publicou o seu parecer 01/2012, lançando o debate sobre a reforma da legislação sobre a proteção de dados.

O grupo, no referido parecer, congratula-se com as soluções apresentadas no que diz respeito ao aumento da responsabilidade dos controladores e o fortalecimento da posição das autoridades de supervisão, quer a nível nacional, quer a nível internacional. Face a esta posição, em junho do mesmo ano, é nomeado Jan Philipp Albrecht como relator do Parlamento Europeu para o Regulamento Geral de Proteção de Dados.

Proceder à alteração da legislação existente e proceder à harmonização das normas em termos europeus foi um percurso difícil

Em janeiro de 2015, o relator e deputado alemão do Parlamento Europeu informou que a legislação sobre a proteção de dados poderia sofrer um atraso até à sua publicação e que a probabilidade de ela ser publicada apenas em 2016 era muito grande. Como se não bastassem todas as pressões exteriores, dentro da União, alguns Estados-membros, como o caso da Alemanha, França e Reino Unido, estavam a exercer uma enorme pressão sobre a necessidade de se alterarem algumas normas do projeto. Só seis meses depois é que se conseguiu almejar um consenso político e global sobre o GDPR e iniciaram-se os trabalhos de elaboração do texto, na sua versão final, com representantes do Parlamento Europeu, do Conselho e da Comissão Europeia.

O percurso continuaria a ser tortuoso e continuou agora o grupo de trabalho a ser pressionado por diversos grupos de empresário, nomeadamente para se alterar o artigo 43º do projeto. Além disso, as declarações polémicas da Procuradora-Geral dos Estados Unidos, Loretta Lynch, que advertiu que a pretensa reforma da proteção de dados europeia poderia ter como consequência a restrição da partilha de informação transatlântica num momento em que todos os esforços estavam a ser desenvolvidos para serem evitados os ataques terroristas.

Apesar disso, finalmente, a 15 de dezembro de 2015 foi alcançado um acordo entre os representantes da Comissão Europeia, do Conselho Europeu e do Parlamento Europeu, tendo sido formalmente aprovada na LIBE o resultado de tais negociações a 17 de dezembro[10].

O Regulamento (EU) 2016/679, do Parlamento e do Conselho, viria a ser aprovado a 27 de abril de 2016 e publicado a 4 de maio do mesmo ano.

O diploma revoga a Diretiva 95/46/CE a partir de 25 de maio de 2018, data em que passará a ser aplicável no ordenamento jurídico europeu, nos termos do disposto no artigo 99º do diploma.

2. Principais novidades

O GDPR é um texto longo, com 173 considerandos e 99 artigos, em que, para a compreensão de algumas normas os considerandos são absolutamente fundamentais. Debruçar-nos-emos, atento os objetivos deste trabalho, nas principais alterações introduzidas pelo GDPR.

É de salientar ainda que o legislador europeu permitiu que o legislador nacional tomasse posição sobre determinadas matérias, como é o caso, nomeadamente, das matérias em sede laboral[11], em que é permitido que os Estados-membros regulem tais questões, sobretudo tendo em atenção a possibilidade de tais matérias virem a ser reguladas através de convenções coletivas de trabalho.

2.1 Âmbito de aplicação

O GDPR aplica-se ao tratamento[12] de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a ele destinados[13], e ainda se aplica ao tratamento de dados pessoais que ocorram quer dentro, quer fora do território da União Europeia, desde que os dados pertençam a cidadãos europeus ou residentes em território europeu[14].

De fato, esta é uma grande alteração e vem resolver entre nós o problema do alojamento em *cloud* de dados pessoais de cidadãos ou residentes num Estado-membro, mas cujo alojamento estava a ser

efetuado fora do espaço da União. Doravante, as regras do GDPR aplicar-se-ão também nestas situações, saindo os interesses dos titulares dos dados pessoais manifestamente reforçados.

Por certo, todo o GDPR é desenvolvido no sentido de que os dados pessoais, não obstante estarem a ser tratados e terem sido recolhidos por uma determinada organização, pertencem ao seu titular e nessa medida é o titular, dos dados pessoais que vai ter sempre a possibilidade de controlar o que acontece aos seus dados, como veremos.

O próprio GDPR define o que são dados pessoais no artigo 4º – trata-se de toda a informação relativa a uma pessoa singular identificada ou identificável. Sendo que, para efeitos do GDPR, é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

2.2 Princípios fundamentais

O artigo 5º, ao estabelecer os princípios fundamentais relativos aos dados pessoais, é considerado uma das principais normas do GDPR.

É expressamente consagrado que a recolha de dados pessoais só poderá existir com fins específicos, além de se estabelecer a minimização dos dados, ou seja, a recolha dos dados deve limitar-se ao estritamente necessário e para um fim em concreto. A consagração de tal princípio vai obrigar a que as organizações, entre nós, alterem radicalmente a sua forma de recolha e tratamento dos dados. Em Portugal é muito habitual para a celebração de um qualquer negócio jurídico serem pedidos ao titular mais dados que aqueles que são estritamente necessários tendo em vista o negócio que está a ser celebrado.

Além disso, consagra o GDPR o princípio da limitação da conservação, ou seja, os dados deverão ser conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados. Depois de tal momento acontecer, os dados deverão ser destruídos. Também aqui a mudança de atitude, nomeadamente no nosso ordenamento

jurídico, será grande. Todos sabemos que uma vez prestados os nossos dados pessoais, estes mantêm-se na organização para eventual uso posterior.

Prevê-se, no entanto, que os dados pessoais possam ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos[15]. Quando tal suceda, os dados estão sujeitos à aplicação de todas as medidas técnicas e organizativas adequadas, tendo em vista a salvaguarda dos direitos e liberdades do titular dos dados.

O que prevê o GDPR nessas circunstâncias é que poderá existir, por exemplo, a pseudonimização[16] dos dados, por forma a permitir que continuem na posse da organização – os dados são tratados de forma a que deixam de poder ser atribuídos a um titular de dados específico. Para isso, a organização terá de assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.

É ainda estabelecido que o processo de recolha de dados tem de ser transparente, leal e lícito. Ora, para que os dados possam ser tratados de forma lícita[17], tem o titular dos dados de consentir para que a recolha se processe.

2.3 O consentimento

O consentimento[18] deve agora ser dado de forma expressa, clara, de modo inteligível, de fácil acesso e numa linguagem clara. O próprio GDPR define o consentimento do titular de dados como uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento[19].

Isso significa que o consentimento tácito, até agora muito usual entre nós, deixa de ser possível. Terá, por um lado, o titular dos dados pessoais de ter a possibilidade de selecionar a finalidade para a qual dá o consentimento para o tratamento dos seus dados pessoais e, por outro lado, tem o direito de retirar o seu consentimento a qualquer momento. De salientar que essa retirada de consentimento tem de ser tão fácil de retirar como foi a de dar[20].

Esta alteração na forma de prestar consentimento terá como principais alterações, desde logo, a proibição de caixas pré-selecionadas no momento da recolha de dados. O titular tem de declarar de forma expressa que autoriza e permite a recolha e o tratamento dos seus dados pessoais.

Uma vez que passa o titular dos dados a ter o verdadeiro poder sobre os mesmos, devem ser previstas regras para facilitar o exercício pelo titular dos direitos que lhe são conferidos ao abrigo do GDPR, incluindo procedimentos para solicitar e, sendo caso disso, obter a título gratuito, em especial, o acesso a dados pessoais, a sua retificação ou o seu apagamento[21] e o exercício do direito de oposição.

O responsável pelo tratamento deverá fornecer os meios necessários para que os pedidos possam ser apresentados por via eletrónica, em especial quando os dados sejam também tratados por essa via. O responsável pelo tratamento deverá ser obrigado a responder aos pedidos do titular dos dados sem demora injustificada e o mais tardar no prazo de um mês e expor as suas razões quando tiver intenção de recusar o pedido, nos termos do disposto no artigo 12º, n. 3, GDPR.

2.4 Os dados sensíveis

O regulamento prevê a proibição de tratamento para aquilo que ele designa de categorias especiais de dados, e isto porque, no que diz respeito aos dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos[22], dados biométricos[23] para identificar uma pessoa de forma inequívoca, dados relativos à saúde[24] ou dados relativos à vida sexual ou orientação sexual de uma pessoa, o tratamento de dados é proibido.

No entanto, está prevista a possibilidade de derrogação à proibição de categorias especiais de dados caso tal seja do interesse público, nomeadamente o tratamento de dados pessoais em matéria laboral, de direito de proteção social, incluindo as pensões, e para fins de segurança, monitorização e alerta em matéria de saúde, prevenção ou controlo. Prevê o GDPR que tais derrogações sejam previstas, especialmente por razões de saúde pública.

No que aos dados de saúde diz respeito, prevê o GDPR que seja realizado o tratamento sem consentimento do titular dos dados quando estejam em causa fins de interesse público, ou de saúde pública, sendo que se entende por saúde pública[25] todos os elementos relacionados com a saúde, ou seja, o estado de saúde, incluindo a morbilidade e a incapacidade, as determinantes desse estado de saúde, as necessidades de cuidados de saúde, os recursos atribuídos aos cuidados de saúde, a prestação de cuidados de saúde e o acesso universal a eles, assim como as despesas e o financiamento dos cuidados de saúde, e as causas de mortalidade. Tais atividades de tratamento de dados sobre a saúde autorizadas por motivos de interesse público não deverão ter por resultado que os dados sejam tratados para outros fins por terceiros, como os empregadores ou as companhias de seguros e entidades bancárias.

2.5 A informação e o acesso aos dados pessoais

Atento o disposto no artigo 13º do GDPR, e nomeadamente nos termos do disposto no artigo 14º do GDPR, o titular dos dados tem de ser informado da operação de tratamento de dados e das suas finalidades. O responsável pelo tratamento deverá fornecer ao titular as informações adicionais necessárias para assegurar um tratamento equitativo e transparente dos dados, tendo em conta as circunstâncias e o contexto específicos em que os dados pessoais forem tratados.

As informações sobre o tratamento de dados pessoais relativos ao titular dos dados deverão ser a este fornecidas no momento da sua recolha junto do titular dos dados ou, se os dados pessoais tiverem sido obtidos a partir de outra fonte, dentro de um prazo razoável, consoante as circunstâncias.

Sempre que os dados pessoais forem suscetíveis de ser legitimamente comunicados a outro destinatário, o titular dos dados deverá ser informado aquando da primeira comunicação dos dados pessoais a esse destinatário, e sempre que o responsável pelo tratamento tiver a intenção de tratar os dados pessoais para outro fim que não aquele para o qual tenham sido recolhidos, antes o responsável pelo tratamento deverá fornecer ao titular dos dados informações sobre esse fim e outras informações necessárias.

O direito de acesso aos dados pessoais recolhidos que lhes digam respeito passa a estar expressamente previsto no artigo 15º do GDPR e tem o titular dos dados a possibilidade de exercer esse direito com facilidade e a intervalos razoáveis, a fim de conhecer o tratamento e verificar a sua licitude.

Não podemos olvidar que o GDPR, ao consagrar o princípio da minimização dos dados, vem impor a obrigação de ser prestado ao titular a informação referente às finalidades para as quais os dados pessoais são tratados, quando possível, ao período durante o qual os dados são tratados, à identidade dos destinatários dos dados pessoais, à lógica subjacente ao eventual tratamento automático dos dados pessoais e, pelo menos quando tiver por base a definição de perfis, às suas consequências.

Este direito de acesso poderá levar a que o titular dos dados requeira, nos termos do disposto no artigo 16º do GDPR, a retificação dos seus dados, quando estes estiverem incompletos ou incorretos.

2.6 O direito ao esquecimento

Este direito ao esquecimento é de fato uma das principais novidades do regulamento, sendo que há muito que se falava deste direito, nomeadamente depois do célebre caso Google[26].

O que determinou o TJUE a 13 de maio de 2014 foi que "prevalecem, em princípio, não só sobre o interesse económico do operador do motor de busca mas também sobre o interesse desse público em encontrar a referida informação durante uma pesquisa sobre o nome dessa pessoa. No entanto, não será esse o caso se se afigurar que, por razões especiais como, por exemplo, o papel desempenhado por essa pessoa na vida pública, a ingerência nos seus direitos fundamentais é justificada pelo interesse preponderante do referido público em ter acesso à informação em questão em virtude dessa inclusão e que o tratamento de dados pessoais (…), realizado pelo operador de um motor de busca, é suscetível de afetar significativamente os direitos fundamentais ao respeito pela vida privada e à proteção de dados pessoais, quando a pesquisa através desse motor seja efetuada a partir do nome de uma pessoa singular, uma vez que o referido tratamento permite a qualquer internauta obter, com a lista de resultados, uma visão

global estruturada das informações sobre essa pessoa, que se podem encontrar na Internet, respeitantes, potencialmente, a numerosos aspetos da sua vida privada e que, sem o referido motor de busca, não poderiam ou só muito dificilmente poderiam ter sido relacionadas, e, deste modo, estabelecer um perfil mais ou menos detalhado da pessoa em causa. Além disso, o efeito de ingerência nos referidos direitos da pessoa em causa é multiplicado devido ao importante papel desempenhado pela Internet e pelos motores de busca na sociedade moderna, que conferem caráter de ubiquidade às informações contidas numa lista de resultados deste tipo."[27]

O que se determina doravante é que qualquer titular de dados tem direito a que os seus dados pessoais sejam apagados e deixem de ser objeto de tratamento, desde que deixem de ser necessários para a finalidade para a qual foram recolhidos ou tratados, se os titulares dos dados retirarem o seu consentimento ou se opuserem ao tratamento de dados pessoais que lhes digam respeito ou se o tratamento dos seus dados pessoais não respeitar o disposto no presente regulamento.

Esse direito assume particular importância quando o titular tiver dado o seu consentimento quando era criança e não estava totalmente ciente dos riscos inerentes ao tratamento, e mais tarde deseje suprimir esses dados pessoais, especialmente na internet.

O titular dos dados deverá ter a possibilidade de exercer esse direito independentemente do fato de já ser adulto. No entanto, o prolongamento da conservação dos dados pessoais deverá ser efetuado de forma lícita quando tal se revele necessário para o exercício do direito de liberdade de expressão e informação, para o cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, por razões de interesse público[28] no domínio da saúde pública, para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

2.7 Data breach

O artigo 32º do GDPR determina que devem ser adotadas as medidas adequadas e oportunas tendo em vista o tratamento dos dados, uma vez que a violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares, como a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social significativa das pessoas singulares.

Caso venha a ocorrer uma violação de dados pessoais, o denominado *data breach*, deverá o responsável pelo tratamento notificar a mesma à autoridade de controlo, sem demora injustificada e, sempre que possível, no prazo de 72 horas após ter tido conhecimento do ocorrido, a menos que seja capaz de demonstrar, em conformidade com o princípio da responsabilidade, que essa violação não é suscetível de implicar um risco para os direitos e liberdades das pessoas singulares.

Se não for possível efetuar essa notificação no prazo de 72 horas, a notificação deverá ser acompanhada dos motivos do atraso, podendo as informações ser fornecidas por fases sem demora injustificada.

Terá também o responsável de comunicar, atento o disposto no artigo 34º do GDPR, a violação de dados pessoais ao titular dos dados sem demora justificada. Esta comunicação deverá descrever a natureza da violação de dados pessoais e dirigir recomendações à pessoa singular em causa para atenuar potenciais efeitos adversos e deverá ser efetuada logo que seja razoavelmente possível, em estreita cooperação com a autoridade de controlo e em cumprimento das orientações fornecidas por esta ou por outras autoridades competentes, como as autoridades de polícia. Por exemplo, a necessidade de atenuar um risco imediato de prejuízo exigirá uma pronta comunicação aos titulares dos dados, mas a necessidade de aplicar medidas adequadas contra violações de dados pessoais recorrentes ou similares poderá justificar um período mais alargado para a comunicação.

Há que verificar se foram aplicadas todas as medidas tecnológicas de proteção e de organização para apurar imediatamente a ocorrência de uma violação de dados pessoais e para informar rapidamente a autoridade de controlo e o titular. Para comprovar que a notificação foi enviada sem demora injustificada importa ter em consideração, em especial, a natureza e a gravidade da violação dos dados pessoais e as respectivas consequências e efeitos adversos para o titular dos dados. Essa notificação poderá resultar numa intervenção da autoridade de controlo em conformidade com as suas funções e competências, definidas pelo presente regulamento.

Ao estabelecer regras pormenorizadas relativamente ao formato e aos procedimentos aplicáveis à notificação das violações de dados pessoais, deverá ter-se devidamente em conta as circunstâncias dessa violação, nomeadamente a existência ou não de proteção dos dados pessoais através de medidas técnicas de proteção adequadas para reduzir eficazmente a probabilidade de usurpação da identidade ou outras formas de utilização abusiva. Além disso, tais regras e procedimentos deverão ter em conta os legítimos interesses das autoridades de polícia nos casos em que a divulgação precoce de informações possa dificultar desnecessariamente a investigação das circunstâncias da violação de dados pessoais.

2.8 A avaliação de impacto

A Diretiva 95/46/CE estabelece uma obrigação geral de notificação do tratamento de dados pessoais às autoridades de controlo. Além de esta obrigação originar encargos administrativos e financeiros, nem sempre contribuiu para a melhoria da proteção dos dados pessoais, tal como é reconhecido nos considerandos do GDPR. Isto levou a que a opção do legislador europeu fosse no sentido de suprimir e substituir tais procedimentos com uma avaliação de impacto sobre a proteção de dados, nos termos do disposto no artigo 35º do GDPR. Esta avaliação de impacto ocorrerá nas operações de tratamento suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, devido à sua natureza, âmbito, contexto e finalidades, nomeadamente quando a operação envolva a utilização de novas tecnologias.

Nesses casos, o responsável pelo tratamento deverá proceder, antes do tratamento, a uma avaliação do impacto sobre a proteção de dados, a fim de avaliar a probabilidade ou gravidade particulares do elevado risco, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento e as fontes do risco. Essa avaliação do impacto deverá incluir as medidas, garantias e procedimentos previstos para atenuar esse risco, assegurar a proteção dos dados pessoais e comprovar a observância do presente regulamento.

Tal deverá aplicar-se às operações de tratamento de grande escala que visem o tratamento de uma grande quantidade de dados pessoais a nível regional, nacional ou supranacional, que possam afetar um número considerável de titulares de dados e que sejam suscetíveis de implicar um elevado risco, por exemplo, em razão da sua sensibilidade, nas quais, em conformidade com o nível de conhecimentos tecnológicos alcançado, seja utilizada em grande escala uma nova tecnologia, bem como a outras operações de tratamento que impliquem um elevado risco para os direitos e liberdades dos titulares dos dados, em especial quando tais operações dificultem aos titulares o exercício dos seus direitos.

É igualmente exigida uma avaliação do impacto sobre a proteção de dados para o controlo de zonas acessíveis ao público em grande escala, nomeadamente se forem utilizados mecanismos optoeletrónicos, ou para quaisquer outras operações quando a autoridade de controlo competente considere que o tratamento é suscetível de implicar um elevado risco para os direitos e liberdades dos titulares dos direitos, em especial por impedirem estes últimos de exercer um direito ou de utilizar um serviço ou um contrato, ou por serem realizadas sistematicamente em grande escala[29].

Sempre que uma avaliação de impacto relativa à proteção de dados indicar que o tratamento, na falta de garantias e de medidas e procedimentos de segurança para atenuar os riscos, implica um elevado risco para os direitos e liberdades das pessoas singulares e o responsável pelo tratamento considerar que o risco não poderá ser atenuado através de medidas razoáveis, atendendo à tecnologia disponível e aos custos de aplicação, a autoridade de controlo deverá ser consultada antes de as atividades de tratamento terem início[30].

2.9 O encarregado de proteção de dados

A figura do encarregado de proteção de dados, comumente designado de DPO, está consagrada no artigo 37º do GDPR. Será obrigatório sempre que o tratamento dos dados for efetuado por uma autoridade pública, com exceção dos tribunais ou de autoridades judiciais independentes no exercício da sua função jurisdicional.

No setor privado, sempre que for efetuado por um responsável pelo tratamento cujas atividades principais consistam em operações de tratamento que exijam o controlo regular e sistemático do titular dos dados em grande escala, ou sempre que as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados pessoais e de dados relacionados com condenações penais e infrações, o responsável pelo tratamento destes ou o subcontratante pode ser assistido por um especialista em legislação e prática de proteção dados no controlo do cumprimento do presente regulamento a nível interno.

No setor privado, as atividades principais do responsável pelo tratamento dizem respeito às suas atividades primárias e não estão relacionadas com o tratamento de dados pessoais como atividade auxiliar.

O nível necessário de conhecimentos especializados deverá ser determinado, em particular, em função do tratamento de dados realizado e da proteção exigida para os dados pessoais tratados pelo responsável pelo seu tratamento ou pelo subcontratante.

Estes encarregados da proteção de dados, sejam ou não empregados do responsável pelo tratamento, deverão estar em condições de desempenhar as suas funções e atribuições com independência.

2.10 As autoridades de controlo independentes

Determina o artigo 51º do GDPR que os Estados-membros deverão criar autoridades de controlo, podendo, se for caso disso, criar mais do que uma autoridade de controlo, de modo a refletir a sua estrutura constitucional, organizacional e administrativa.

Em Portugal a nossa autoridade de controlo é a Comissão Nacional de Proteção de Dados, que existe desde 7 de janeiro de 1994.

Ora, deverão as autoridades de controlo serem dotadas de recursos financeiros e humanos e de infraestruturas necessárias ao desempenho eficaz das suas atribuições, incluindo as relacionadas com a assistência e a cooperação mútuas com outras autoridades de controlo da União.

Prevê o GDPR que as condições gerais aplicáveis aos membros da autoridade de controlo deverão ser definidas por lei em cada Estado-membro e deverão prever, em especial, que os referidos membros sejam nomeados, com recurso a um processo transparente, pelo Parlamento, pelo Governo ou pelo Chefe de Estado do Estado-membro com base numa proposta do Governo, de um dos seus membros, do Parlamento ou de uma sua câmara, ou por um organismo independente incumbido da nomeação nos termos do direito do Estado-membro.

Deverão as autoridades de controlo serem dotadas de recursos financeiros e humanos e da infraestrutura necessária ao desempenho eficaz das suas atribuições

A fim de assegurar a independência da autoridade de controlo, os membros que a constituem deverão exercer as suas funções com integridade, abster-se de qualquer ato incompatível com as mesmas e, durante o seu mandato, não deverão exercer nenhuma atividade, seja ou não remunerada, que com elas seja incompatível.

A autoridade de controlo deverá dispor do seu próprio pessoal, selecionado por si mesma ou por um organismo independente criado nos termos do direito do Estado-membro, que deverá estar exclusivamente sujeito à orientação do integrante ou integrantes da autoridade de controlo.

As autoridades de controlo deverão ser competentes no território do respectivo Estado-membro para exercer os poderes e desempenhar as funções que lhes são conferidas nos termos do presente regulamento. Deverão ainda controlar a aplicação das disposições do presente regulamento e contribuir para a sua aplicação coerente em toda a União, a fim de proteger as pessoas singulares relativamente ao tratamento dos seus dados pessoais e facilitar a livre circulação desses dados a nível do mercado interno. Para esse efeito, as autoridades de controlo deverão

cooperar entre si e com a Comissão Europeia, sem necessidade de qualquer acordo entre os Estados-membros quer sobre a prestação de assistência mútua, quer sobre tal cooperação.

A fim de assegurar o controlo e a aplicação coerentes do presente regulamento em toda a União, as autoridades de controlo deverão ter, em cada Estado-membro, as mesmas funções e poderes efetivos, incluindo poderes de investigação, poderes de correção e de sanção, e poderes consultivos e de autorização, nomeadamente em caso de reclamação apresentada por pessoas singulares, sem prejuízo dos poderes das autoridades competentes para o exercício da ação penal ao abrigo do direito do Estado-membro, tendo em vista levar as violações ao presente regulamento ao conhecimento das autoridades judiciais e intervir em processos judiciais. Essas competências deverão incluir o poder de impor uma limitação temporária ou definitiva ao tratamento, ou mesmo a sua proibição.

Os poderes de investigação em matéria de acesso às instalações deverão ser exercidos em conformidade com os requisitos específicos do direito processual do Estado-membro, como, por exemplo, a obrigação de obter autorização judicial prévia.

As medidas juridicamente vinculativas da autoridade de controlo deverão ser emitidas por escrito, claras e inequívocas, indicar a autoridade de controlo que as emitiu e a data de emissão, ostentar a assinatura do diretor ou do membro da autoridade de controlo por eles autorizada, indicar os motivos que as justificam e mencionar o direito de recurso efetivo.

2.11 O Comité Europeu para a Proteção de Dados

O artigo 68º vem prever a criação de comité europeu para a proteção de dados, com o objetivo de promover a aplicação coerente do GDPR. Deverá ser um órgão independente da União e como tal é dotado de personalidade jurídica. Este comité vai substituir o WP 29 da Diretiva de 1995.

O comité deverá contribuir para a aplicação coerente do presente regulamento em toda a União, incluindo o aconselhamento da Comissão, nomeadamente no que respeita ao nível de proteção em países terceiros ou em organizações internacionais, e mediante a

promoção da cooperação das autoridades de controlo em toda a União. O comité deverá ser independente na prossecução das suas atribuições.

2.12 Penalidades

O artigo 79º do GDRP é de fato um dos principais artigos do diploma, porque vem estabelecer que qualquer pessoa que tenha sofrido danos materiais ou imateriais tem direito a ser ressarcida. E determina ainda que qualquer responsável pelo tratamento é responsável pelos danos, sendo-o também o subcontratante, desde que demonstre que não seguiu as instruções lícitas do responsável pelo tratamento.

As coimas podem variar entre 10 000 000EUR, ou no caso de uma empresa até 2 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado, e 20 000 000EUR, ou, no caso de uma empresa, até 4% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado, dependendo da gravidade da infração.

3. Conclusão

Como tivemos oportunidade de analisar, ainda que de forma manifestamente superficial, as alterações trazidas pelo GDPR são inúmeras e ainda se aguarda que os Estados-membros adaptem a sua legislação nacional ao GDPR. A Alemanha é o país europeu que está mais avançado neste processo, bem como a Espanha, cujo diploma está já em fase de discussão pública.

Adivinham-se tempos complicados para as empresas, mas de um enorme reforço dos direitos das pessoas singulares.

Notas

1. O presente texto corresponde, com alguns desenvolvimentos, à nossa comunicação apresentada nas VII Jornadas de Direito do Consumo, que tiveram lugar na Escola Superior de Tecnologia e Gestão do IPLeiria, no dia 9 de março de 2017.
2. Jorge Barros Mendes. Docente na Escola Superior de Tecnologia e Gestão do IPLeiria. Investigador no CIEJE-IPLeiria. Advogado.

3. A sobredita convenção considera que uma das finalidades do Conselho da Europa é conseguir uma união mais estreita entre os seus membros, nomeadamente no respeito pela supremacia do direito, bem como dos direitos do homem e das liberdades fundamentais.
4. Doravante designado abreviadamente por TJUE.
5. TJUE, acórdão de 24 de novembro de 2011 – processos apensos C-468/10 e C-469/10, Asociación Nacional de Estalecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estad, n. 28 e 29.
6. (2000/C 364/01) JOCE de 18.12.2000.
7. Comumente designado por GDPR, terminologia que adotaremos doravante.
8. Designado doravante como WP29.
9. LIBE.
10. Com uma maioria esmagadora (quarenta e oito votos a favor, quatro contra e quatro abstenções), a comissão LIBE aprovou o texto final do GDPR, incluindo disposições sobre o consentimento claro e afirmativo, as crianças nas redes sociais, o direito ao esquecimento, o direito da pessoa singular ser informada quando exista violação dos seus dados pessoais, a utilização de uma linguagem simples e multas de até 4% do volume de negócios total anual mundial das empresas.
    Em 18 de dezembro de 2015, o Comité dos Representantes Permanentes (COREPER) confirmou com esmagadora maioria (apenas um voto contra) os textos de compromisso acordados pelo Conselho, pelo Parlamento e pela Comissão em 15 de dezembro.
11. Cfr. artigo 88º do GDPR.
12. Atento o disposto no artigo 4º, n. 2, da DDPR, tratamento é: uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.
13. Cfr. artigo 2º GDPR. Deverá ter-se em atenção que qualquer organização que detenha um simples ficheiro word ou excel que contenha dados de natureza pessoal, ou um simples arquivo em papel deverá, como veremos, de cumprir com as obrigações impostas pelo GDPR. Para o diploma, atento o disposto no n. 6 do artigo 4º, é considerado ficheiro qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico.
14. Cfr. artigo 3º GDPR.
15. Cfr. artigo 89º GDPR. O artigo 89º é uma das normas que se espera que venha a ser objeto de regulamentação pelo legislador nacional.
16. Cfr. artigo 4º, n. 5, GDPR.
17. Cfr. artigo 6º GDPR.

18. Cfr. artigo 7º GDPR.
19. Cfr. artigo 4º, n. 11, GDPR.
20. Cfr. artigo 7º, n. 3, GDPR.
21. O denominado direito ao esquecimento.
22. Nos termos do artigo 4º, n. 13, do GDPR, são considerados dados genéticos os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa.
23. Nos termos do artigo 4º, n. 14, são considerados dados biométricos os dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos.
24. Nos termos do artigo 4º, n. 15, são considerados dados de saúde os dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde.
25. Nos termos do Regulamento (CE) n. 1338/2008, do Parlamento Europeu e do Conselho.
26. Caso Google, Assunto C-11/12 – Em 5 de março de 2010, M. Costeja González, de nacionalidade espanhola e domiciliado em Espanha, apresentou na autoridade administrativa espanhola – AEPD – uma reclamação contra a La Vanguardia Ediciones SL, que publica um jornal de grande tiragem, designadamente na Catalunha, o "La Vanguardia", e contra a Google Spain e a Google Inc. Esta reclamação baseava-se no fato de que, quando um internauta inseria o nome de M. Costeja González no motor de busca do grupo Google, obtinha ligações a duas páginas do jornal da La Vanguardia de, respectivamente, 19 de janeiro e 9 de março de 1998, nas quais figurava um anúncio de uma venda de imóveis em hasta pública decorrente de um arresto com vista à recuperação de dívidas à Segurança Social, que mencionava o nome de M. Costeja González.
    Com esta reclamação, M. Costeja González pedia, por um lado, que se ordenasse à La Vanguardia que suprimisse ou alterasse as referidas páginas, para que os seus dados pessoais deixassem de aparecer, ou que utilizasse determinadas ferramentas disponibilizadas pelos motores de busca para proteger esses dados, e por outro lado pedia que se ordenasse à Google Spain ou à Google Inc. que suprimissem ou ocultassem os seus dados pessoais, para que deixassem de aparecer nos resultados de pesquisa e de figurar nas ligações da La Vanguardia.
    E isto porque o processo de arresto, de que fora objeto, tinha sido completamente resolvido há vários anos e a referência ao mesmo carecia atualmente de pertinência.
    Sucede que a autoridade administrativa espanhola – AEPD –, por decisão de 30 de julho de 2010, considerou que a reclamação em relação ao jornal à La Vanguardia estava legalmente justificada, dado que tinha sido efetuada por

ordem do Ministério do Trabalho e dos Assuntos Sociais e teve por finalidade publicitar ao máximo a venda em hasta pública, a fim de reunir o maior número possível de licitantes, sendo que, no que concerne à Google, a AEPD considerou que os operadores de motores de busca estão sujeitos à legislação em matéria de proteção de dados, uma vez que realizam um tratamento de dados pelo qual são responsáveis e atuam como intermediários da sociedade de informação.

A AEPD considerou que estava habilitada a ordenar a retirada dos dados e a interdição de aceder a determinados dados, por parte dos operadores de motores de busca, quando considere que a sua localização e a sua difusão são suscetíveis de lesar o direito fundamental de proteção dos dados e a dignidade das pessoas em sentido amplo, o que abrange também a simples vontade da pessoa interessada de que esses dados não sejam conhecidos por terceiros. A AEPD considerou que esta obrigação pode incumbir diretamente aos operadores de motores de busca, sem que seja necessário suprimir os dados ou as informações do sítio *web* onde figuram, designadamente quando a manutenção dessas informações nesse sítio seja justificada por uma disposição legal.

27. Cfr. parágrafo 80 e 97 do referido acórdão.
28. Em acórdão recente, de 9 de março de 2017, Proc. C-398/15, o TJEU considerou que os dados pessoais que são inscritos no registo das sociedades possam ser, após um determinado período de tempo e a pedido da pessoa em causa, cancelados, tornados anónimos ou bloqueados, ou tornados acessíveis a um círculo restrito de terceiros, a saber, os terceiros que justifiquem um interesse legítimo no acesso a esses dados.
29. O tratamento de dados pessoais não deverá ser considerado de grande escala se disser respeito aos dados pessoais de pacientes ou clientes de um determinado médico, profissional de cuidados de saúde, hospital ou advogado. Nesses casos, a realização de uma avaliação de impacto sobre a proteção de dados não deverá ser obrigatória.
30. No âmbito desse processo de consulta, o resultado de uma avaliação do impacto sobre a proteção de dados efetuada relativamente ao tratamento em questão pode ser apresentado à autoridade de controlo, em especial as medidas previstas para atenuar o risco para os direitos e liberdades das pessoas singulares.